International Journal of Computer Applications Technology and Research
Volume 5– Issue 7, 417 - 421, 2016, ISSN:- 2319–8656

Development of Computational Tool for Lung Cancer Prediction Using Data Mining

Divya Chauhan
Shoolini University
Solan, Himachal Pradesh
India

Varun Jaiswal
Shoolini University
Solan, Himachal Pradesh
India

Abstract: The requirement for computerization of detection of lung cancer disease arises ever since recent-techniques which involve manual-examination of the blood smear as the first step toward diagnosis. This is quite time-consuming, and their accurateness depends upon the ability of operator's. So, prevention of lung cancer is very essential. This paper has surveyed various techniques used by previous authors like ANN (Artificial Neural Network), image processing, LDA (Linear Dependent Analysis), SOM (Self Organizing Map) etc.

Keywords: Lung Cancer, Classification, Neural Network, SOM, LDA, PCA, Chi-Square, Feature Extraction.

1. INTRODUCTION

1.1 Background

Lung cancer research is one of the most concerning area of interest in medical field. The early diagnose of the cancer can help in increasing the mortality rate of humans [1]. Lung cancer is customarily a contagion which takes place because of the element linked with unimpeded cell or conveniently progress in zones present in lung area. According to American Cancer Society it is approximated that 48,610 persons (27,880 men and 20,730 women) will be detected with and 23,720 men and women will have high percentage of lung cancer in 2013 only [2]. In turn, it is part of the even broader set of diseases disturbing the tuberculosis, Silicosis and Interstitial Lung Disease (ILD), which are all known as diffuse parenchymal lung disease (DPLD) [3].

1.2 Data Mining in Medical Field

Data mining is the process in which valuable information is extracted from the large dataset. It has reached the high growth over past few years. Due to the usefulness of data mining approaches in health world, it has become the good technology in healthcare domain [4]. This realization leads to explosion of data mining approaches [5]. Medical data mining can exploit the hidden patterns present in voluminous medical data which otherwise is left undiscovered. Data mining techniques which are applied to medical data include association rule mining for finding frequent patterns, prediction, classification and clustering. Traditionally data mining techniques were used in various domains. However, it is introduced relatively late into the Healthcare domain [6]. Nevertheless, as on today lot of research is found in the literature. This has led to the development of intelligent systems and decision support systems in Healthcare domain for accurate diagnosis of diseases, predicting the severity of various diseases, and remote health monitoring. Especially the data mining techniques are more useful in predicting heart diseases, lung cancer, and breast cancer and so on.

1.3 CET Images and its Importance in Medical Field

A CET scanner uses the digital processing to get 3-D image of an object [7]. A CET scanner emits the radiation from a device then scans the whole body to get 3-D image [8]. CET scan is very important as CET scans are a valuable diagnostic tool. They are able to detect some conditions that conventional XY-rays cannot, since CET scans can show a "3-D" view of the section of the body being studied. CET scans are also useful for monitoring a patient's progress during or after treatment [9].

In this paper, various techniques to detect lung cancer will be presented along with brief outline of lung cancer detection.

2. RELATED WORK

Hossein GhayoumiZadeh, et al. [10], 2013 represented an image analysis approach for automated detection, preprocessing-smoothing, enhancement, segmentation, feature extraction-morphological and calorimetric and then detection and categorization of particular cells, particularly the cancer cells from usual cells is complete.

Lim Huey Nee, et al. [11], 2012 presented the incline scale, thresholding, morphological operation and division change to perform cell segmentation. In this paper 50 imageries were used to test the planned method and the effect showed that the process hasmanaged to obtain qualitatively good segmentation consequences.

FauziahKasmin [12], 2012 presented the recognition of blood disorder is through visual inspection of tiny images of blood cells. From the recognition of blood disorders, it can lead to classification of certain diseases related to blood. This document describes a first round study of developing a detection of leukemia types using microscopic blood sample imagery. Here, analyzing through images is very significant as from images; disease can be detected and diagnosed at earlier stage. From there, further actions like scheming, monitoring and prevention of diseases can be done. Imagery is used as they are despicable and do not need expensive testing and lab equipment’s. The system will focus on white blood cells disease, leukemia. The system will use features in microscopic images and look at changes on texture, geometry, color and statistical analysis. Changes in these features will be used as a classifier input. A text appraisal has been done and Reinforcement Learning is proposed to classify types of leukemia. A small conversation about issues concerned by researchers also has been ready.

WaidahIsmail [13], 2011 presented a method for the detection and classification of blast cells in M3 with others sub types using computer generated annealing and neural networks. In this paper, we greater than before our test result from 10 images to 20 images. We perform Hill Climbing; Simulated Annealing and Genetic Algorithms for detect the blast cells. As a result, simulated annealing is the "best" heuristic search for detecting the leukemia cells. From the detection, we perform features extraction on the blast cells and we classify based on M3 and other sub-types using neural networks. We received persuasive result which has targeting around 97% in classify of M3 with other sub-types. Our consequences are based on real world image data from a Hematology Department

3. VARIOUS TECHNIQUES FOR CANCER DETECTION AND PREVENTION

3.1 ANN (Artificial Neural Network)

An artificial neural network does not shot to be like the thought process and if/ then sense of the people brain as completed by an expert system. It mimics exact aspects of the in turn dispensation and objective sympathetic of the brain by means of a network of neural link [14]. As a result, a number of writers record it as a "microscopic", "white box" structure and a professional system as a "macroscopic", "black box" system. An Artificial Neural Network consists of a huge amount of simple dispensation elements that are dependable and covered [15].

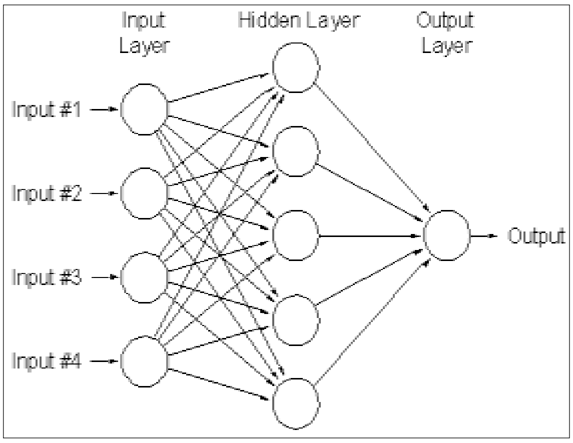


Figure 1: Basic Diagram of A.N.N

Inputs: x1, x2, x3, x4……………………….xn

Weights: w1j, w2j, w3j, w4j………………..wnj

TransferFunction: ∑

Activation Function: α

Output: x1w1j, x2w2jj…………….xnwnj

3.2 LDA (Linear Dependent Analysis)

Linear Discriminant Analysis is utmost commonly utilized as dimensionality lessening method in the pre-processing stage for machine learning applications in addition to design-classification. The main objective is to project a specific dataset on top of a lower-dimensional space using virtuous class reparability so as to decrease computational prices as well as also evade overfitting [16]. The novel linear discriminant was first designated for a two-class issue, in addition it was then afterwards widespread as "Multiple Discriminant Analysis" or "multi-class LDA" through C. R. Rao in the year of 1948. Linear Discriminant Analysis is "controlled" as well as calculates the guidelines ("linear discriminants") which would probably signify the axes that are applied to make the most of the separation amongst multiple type of classes. Below are the five basic steps utilized for implementing a LDA technique [17].

A necessary and sufficient condition for the set of functions:

$f_1(x)$, $f_2(x)$...fn(x) to be linearly independent is that

$c_1 f_1(x) + c_2 f_2(x) + ... + c_n f_n(x) = 0$

only when all the scalars c_i are zero.

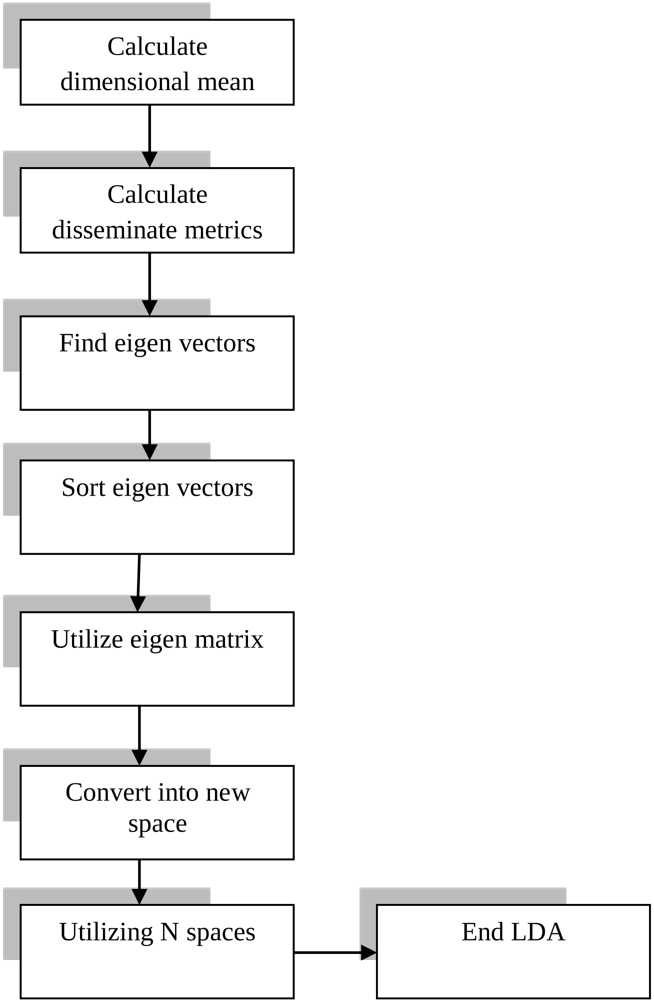


Figure 2: Basic Diagram of L.D.A

3.3 Self-Organizing Map (SOM)

The Self-Organizing Map is one of the commonly used network model. It belongs to the learning networks. The Self-Organizing Map is un-supervised learning method. If Self-Organizing Map is used for feature extraction then it is called Self-Organizing Feature Map [18].

Below figure shows that there are 5 cluster units, Yi and 7 input units, Xi. Clusters are arranged in linear array [19].

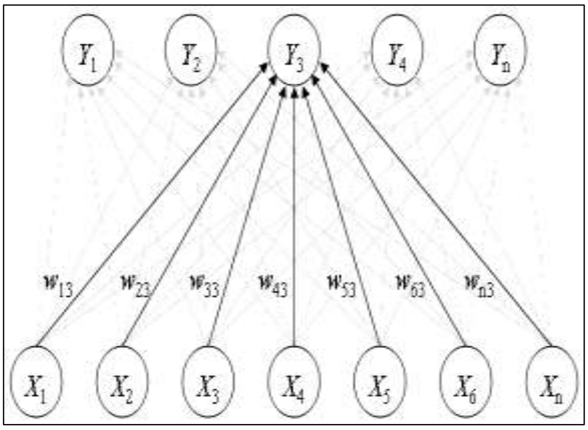


Figure 3: SOM Example

Self-Organizing Map was designed by Kohonen. The SOM has been useful in many applications. It maps the high dimensional space to map units for preserve mapping. Neuron units commonly made lattice onto a plane. Preserving property means reserving the distance between points. In addition to that Self-Organizing Map has the capability of generalizing. It means recognizing the patterns that never met before. The Self-Organizing Map I 2-D can be represented as following**:**

$$Y = \{ x......x_{acw} \} \qquad (1)$$

The neurons are connected to adjacent neurons by a relation. Commonly, the neurons are connected to each other via rectangular or hexagonal topology. Topologies of neurons are represented above.

Randomly choose a vector

Determine output node wi.

wi x >= wk

Weight update is given as below:

w(new) = w(old) + υ

3.4 Support Vector Machines (SVM)

Support Vector Machine (SVM) is first and foremost a classier technique which executes classification tasks through building hyperplanes in a multi-dimensional space, which divides cases of different and dissimilar class labels. We can define the matrix

$(H)_{ij} = y_i y_j (x_i \cdot x_j)$, (2)

And introduce more compact notation [20]:

Minimize:

$W(a) = -a^T 1 + ½ a^T Ha$

Subject to:

$a^T y = 0$

$0 \le a \le C1$

Support Vector machines are also called kernel machines and they have two phases of training:

- Transform input data to high dimensional data.
- Solve quadratic problem [21].

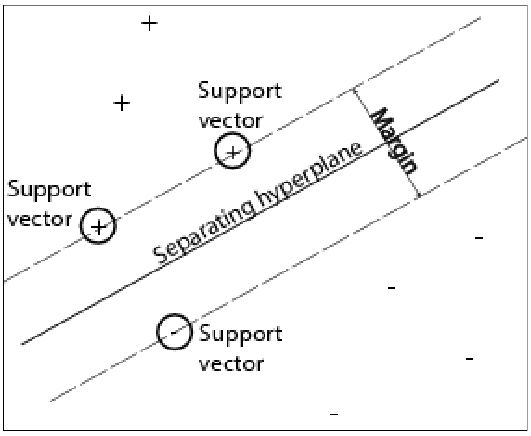


Figure 4: SVM Planar Division

3.5 Genetic Algorithm (GA)

Genetic algorithm is the type of algorithm that is used to solve both constrained and non-constraint problems based on selection criteria. Genetic algorithm modifies the new population and generate new solutions until best solution has not been reached. From large set of population, genetic algorithm uses the random chromosomes to make it parent then make it to produce children [22].

Choose initial population

From left population, select individual chromosomes.

Choose best selected chromosomes

Do crossover

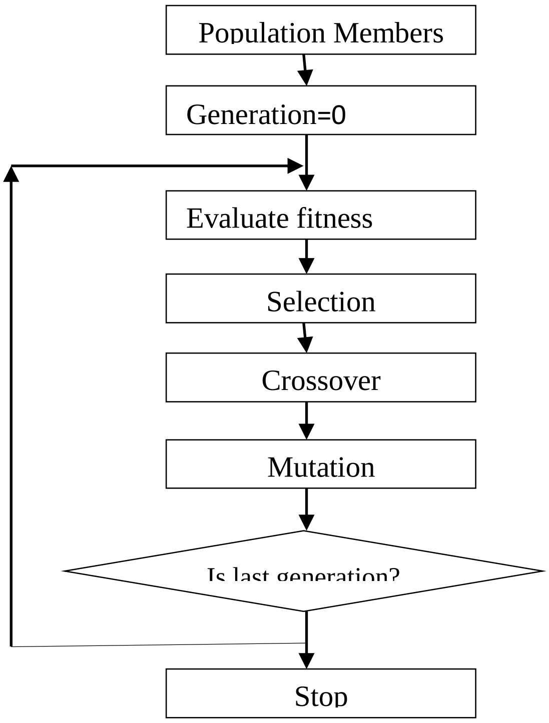
Do repetition

End

Figure 5: Genetic Algorithm Process

3.6 Principal Component Analysis (PCA)

Principal components analysis (PCA) is basically useful for reducing the number of variables that consists a data set while retaining the inconsistency in the data and to identify unknown patterns in the data and to classify them according to how much of the information, stored in the data, they report for [23].



PCA allows calculating a linear alteration that maps information as of a high dimensional space to a lower dimensional space [24].

B1 = t11 a11 +………t1n an

B2 = t21 a1 +………..t2an

Linear transformation implied by PCA

The linear transformation R^N -> R^K3 that performs the dimensionally reduction

B1 U^t1

B2 U^t2 (x- |x|) = U^t (x- |x|)

3.7 Discreet Wavelet Transform (DWT)

With the enlargement in utilization of internet, communication of data has turn out to be quiet easy. In contrast with the data communication in analog form, digital communication offers us several aids for instance enhanced/superior quality, high speed, compression of data etc [25]. However, image acquisition has some shortcomings also, such as the noise present during transmission. The recognition of the specific data is one of the significant necessities in the arena of information transmission, whether it is the transmission of information/data in military-applications or transmission of pictures on internet that desires to be safer than before [26].

The wavelet transform has grown pervasively approval in denoising of image as well as signal processing. It is the breaking down a specific signal into scaled along with shifted versions of the unique wavelet. A wavelet is a type of waveform of efficiently restricted duration which has average value of zero. And for signals; the identity of the specific signal is specified through the component of low-frequency.

We can approximate a discrete signal in k^2 (X) ^{1} by

$$f[b] = \frac{1}{\sqrt{N}}\sum_j Q_\phi[h_0,j]\,\phi_{h_0,j}[b] + \frac{1}{\sqrt{N}}\sum_{h=h_0}^{\infty}\sum_j Q_\psi[h,j]\psi_{h,j}[b](3)$$

Here, $f[b], \phi_{h_0,j}[b]$ and $\psi_{h,k}[b]$ are discrete functions which are defined in [0, N-1], to-tally N points. For the reason that the sets $\{\phi_{h_0,j}[b]\}_{j\in X}$ and $\{\psi_{h,j}[b]\}_{(h,j)\in X^2, h\geq j_0}$ are orthogonal to each other. We can simply take the inner product to obtain the wavelet coefficients:

$$Q_\phi[h_0,j] = \frac{1}{\sqrt{N}}\sum_b f[b]\,\phi_{h_0,j}[b] \qquad (4)$$

$$Q_\psi[h_0,j] = \frac{1}{\sqrt{N}}\sum_b f[b]\,\psi_{h,j}[b] \quad h \geq h_0 \qquad (5)$$

(4) are called approximation coefficients while (5) are called detailed coefficients.

3.8 Chi Square Test Analysis

The chi-squared one-variable test serve a principle comparable to the binomial test, excluding that it can be used when there are more than two categories to the variable. Thus, if you want to resolve if the numbers of people in each of several categories vary from some predict values, the chi-squared one-variable test is proper. The chi-square goodness-of-fit test is a single-sample non-parametric test, also referred to as the one-sample goodness-of-fit test [27].

4. CONCLUSION AND FUTURE SCOPE

Lung cancer is one of the major health problems in all over world. Cancer constitutes 10.3% of medically certified deaths, which is the most leading cause of death after disease of the circulatory system, accidents and disease of the respiratory system. There are over 100 different types of cancer and one of them is lung cancer. In lung cancer treatment delay results in high mortality rate. So, this paper has reviewed cancer cell detection using various methods.

Use of support vector machines will be considered in the future work as a classification tool. Support Vector Machine (SVM) is also called Support Vector Networks are supervised learning models that analyze data and recognize patterns.

5. REFERENCES

[1] Raje, C.; Rangole, J., "Detection of Leukemia in microscopic images using image processing," in Communications and Signal Processing (ICCSP), 2014 International Conference on , vol., no., pp.255-259, 3-5 April 2014.

[2] Kalyanmoy Deb, A. Raji Reddy, “Reliable classification of two-class cancer datausing evolutionary algorithms”, Elsevier, BioSystems , Vol.72, pp.111–129, 2003.

[3] SubrajeetMohapatra, SushantaShekharSamanta, DiptiPatra and SanghamitraSatpathi, “Fuzzy based Blood Image Segmentation for Automated Leukemia Detection”, IEEE, 2012.

[4] Nimesh Patel, AshotoshMehra, “Automated Detection of Leukimiausing microscopic images”, Elsevier, Vo. 58, 2015.

[5] Jafar, I., Hao Ying , Shields ,A.F., Muzik , O. ‘Computerized Detection of Lung Tumors in PET/CT Images’, EMBS 2006, 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2006.

[6] Nakao M, Kawashima A, Kokubo M, Minato K. “Simulating Lung Tumor Motion for Dynamic Tumor-Tracking Irradiation”. Nuclear Science Symposium Conference Record, 2007. NSS 2007

[7] E, Donald, “Introduction to Data Mining for Medical Informatics,” Clin Lab Med, pp. 9-35, 2008.

[8] R. Zhang, Y, Katta, “Medical Data Mining,” Data Miningand Knowledge Discovery, pp. 305-308, 2002.

[9] Irene M. Mullins et al., “Data mining and clinical data repositories: Insights from a667,000 patient data set,” Computers in Biology and Medicine, vol. 36, pp. 1351-1377, 2006.

[10] Zadeh, Hossein Ghayoumi, SiamakJanianpour, and JavadHaddadnia, "Recognition and Classification of the Cancer Cells by Using Image Processing and Lab VIEW," International Journal of Computer Theory and Engineering (2013).

[11] L. H. Nee, M. Y. Mashor, R. Hassan,"White Blood Cell Segmentation for Acute Leukemia Bone Marrow Images," International Conference on Biomedical Engineering (ICoBE),Penang, Malaysia, 27-28 February 2012.

[12] Kasmin, Fauziah, Anton SatriaPrabuwono, and Azizi Abdullah, "Detection ofLeukemia in Human Blood Sample Based On Microscopic Images: A Study, " Journal of Theoretical & Applied Information Technology46.2 (2012).

[13] Ismail, Waidah, et al. "The detection and classification of blast cell in Leukaemia Acute PromyelocyticLeukaemia (AML M3) blood using simulated annealing and neuralnetworks." (2011).

[14] K.A.G. Udeshani, R.G.N. Meegama, T.G.I. Fernando, “Statistical Feature-based Neural Network Approach for the Detection of Lung Cancer in Chest X-Ray Images,” International Journal of Image Processing (IJIP), Volume (5), Issue (4) , 2011.

[15] Jinsa , “Lung cancer classification using neural networks for CT images”, Computer Methods and Programs in Biomedicine, Volume 113, Issue 1, January 2014, Pages 202-209

[16] J. Yang, D. Zhang, J.-Y. Yang and B. Niu , "Globally max-imizing, locally minimizing: unsupervised discriminant projection with applications to face and palm biometrics" , IEEE transactions on pattern analysis and machine intelligence , vol. 29 , no. 4 , pp.650 -664 , 2007

[17] Young Tae Lee; Yong Joon Shin; Cheong Hee Park, "Extending Linear Discriminant Analysis by Using Unlabeled Data," in Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on , vol., no., pp.557-562, Aug. 31 2011-Sept. 2 2011.

[18] C. J. Lin, C.H. Chu, C.Y. Lee, Y.T. Huang, “2D/3D Face Recognition Using Neural Networks Based on Hybrid Taguchi Particle Swarm Optimization”, Eighth International Conference on Intelligent Systems Design and Application (ISDA), 307-312, DOI : 10.1109/ISDA.2008.286.

[19] Timothy Rumbell, Susan L. Denham, and Thomas Wennekers, “A Spiking Self-Organizing Map Combining STDP, Oscillations, and Continuous Learning”, IEEE Transactions On Neural Networks And Learning Systems, Vol. 25, No. 5, May 2014

[20] M. Hearst. Support vector machines. IEEE Transactions on IntelligentSystems, 18 – 28, 1998.

[21] Detection of Lung Nodule Using Multiscale Wavelets and Support Vector Machine. K.P.Aarthy, U.S.Ragupathy

[22] Man, K.F.; Tang, K.S.; Kwong, S., "Genetic algorithms: concepts and applications [in engineering design]," in Industrial Electronics, IEEE Transactions on , vol.43, no.5, pp.519-534, Oct 1996, doi: 10.1109/41.538609.

[23] Taranpreet Singh Ruprah, “Face Recognition Based on PCA Algorithm,” Special Issue of International Journal of Computer Science & Informatics (IJCSI), 2231–5292, Vol.- II, Issue-1, 2

[24] M. Turk and A. Pentland. Eigenfaces for face recognition, "Cognitive Neuroscience Journal," vol. 3, no. 1, pp.71-86, March 1991.

[25] Z. Tufekci and J. N. Gowdy, "Feature extraction using discrete wavelet transform for speech recognition," IEEE Inter.Conf. Southeastcon2000, pp. 116-123, April 2000.

[26] K. P. Soman and K. I. Ramchandran, Insight into Wavelets from Theory to Practice, Printice-Hall of India, 2e, 2005.

[27] Yong Li, "Applications of Chi-Square Test and Contingency Table Analysis in Customer Satisfaction and Empirical Analyses," in Innovation Management, 2009. ICIM '09. International Conference on , vol., no., pp.105-107, 8-9 Dec. 2009

International Journal of Computer Applications Technology and Research
Volume 5– Issue 7, 422 - 432, 2016, ISSN:- 2319–8656

Program Aging and Service Crash

Shahanawaj Ahamad, Ph.D.
Dept. of Computer Sc. & Software
Engineering, College of Computer
Science & Engineering,
University of Ha'il,
Ha'il, K.S.A.

Abstract: Program aging is a degradation of performance or functionality caused by resource depletion. The aging affects the cloud services which provide access to big data bank and computing resources. This suffers large budget and delays of defect removal, which requires other related solutions including renewal in the form of controlled restarts. Collection of various runtime metrics are more significant source for further study of detection and analysis of aging issues. This study highlights the method for detecting aging immediately after their introduction by runtime comparisons of different development scenarios. The study focuses on aging of program and service crash as a consequence.

Keywords: Program; Aging; Cloud service; Renewal, Metrics.

1. INTRODUCTION

Aging occurrence comprises in expansion of crash rate or performance deprivation of computers as it implements, which is due to the collection of faults in computers state and depletion of resources, for example, physical space [1] [2]. This occurrence is known to experts since quite a while. Early indications of software aging were found in 1960s [3]. As programming is growing in size and difficulty, program aging is perceived in expanding number of long-running computers, together with communications. Program aging is accredited to indirect computer program bugs. Researches in early 1990s on telecom computers [6] emphasized high occurrence of viruses and bugs which, when activated, don't instantly bring about program crash, however show themselves as space spillage, lock of unreleased files, corrupted data and accumulation of numerical fault, slowly degrading computers performance and finally to failure. Sometimes such viruses and bugs are too subtle or too expensive, making it impossible to be expelled during improvement. Studies at AT&T Bell laboratories on error enduring program recognized as program renewal as economical solution to counter program Aging [1] [7] [3]. Program renewal is a positive method to prevent performance deprivation and crashes from program aging. It comprises incidental or periodical tidy up of aging impacts (which are accomplished by computer program restart, or by more difficult procedures), so as to delay crashes and reinstate performance. Program renewal represents a unique type of defensive program support contrasted with different types of defensive program upkeep [8], which were centered on to install updates so as to avert field crashes [9] or redesign a package, to adapt to outdated quality [10].

Accuracy of Aging Oriented Crash (AOC) detection approaches is largely determined by aging indicators. A well-designed aging indicator can precisely indicate AOC. If subsequent renewals are always conducted at real crash-prone state, renewal cost will tend to be optimal and significant with optimum schedule. But unfortunately, prior detection approaches based upon explicit aging indicators [11] [12], [13], [14], [15] [16], [17]. These approaches don't function well especially in face of dynamic workloads. Mostly they miss some crashes which lead to a low recall. Insufficiency of previous indicators motivates to seek novel indicators. There are some motivational aspects as follows.

1.1 Insufficiency of Explicit Aging Indicators

To distinguish normal state and crash-prone state, a threshold should be present on aging indicator. Once aging indicator exceeds threshold, a crash occurs. Traditionally, a threshold is set on explicit aging indicators. For instance, if CPU utilization exceeds 90%, a crash occurs. However, it's not always case to happen. External observations do not always reveal accurately internal states. Here internal states are referred to as some normal events (e.g. a file reading, a packet sending) or abnormal events (e.g. a file open exception, a round-off error) generated in computers. Abnormal events are more concerned here. CPU utilization is observed as real number in range 0%, 100% while abnormal events are very limited. Therefore an abnormal event correlates with multiple observations. When a crash-prone event happens, CPU utilization is 99%, 80% or even 10%. Therefore explicit aging indicator cannot signify AOC sufficiently and accurately; and if computers fluctuation is taken into account, situation gets even worse. This is also a reason why it's so difficult to set an optimal threshold on explicit aging indicators in order to obtain an accurate crash detection result.

1.2 Entropy Increase in VoD Computers

As explicit aging indicators fall short in detecting AOC, turning to implicit aging indicators is helpful. Some insights are attained from [18] and [15]. Both of them treated program aging as a complex process. With their motivation it is believed that entropy can be a measurement of complexity, which has a potential to be an implicit aging indicator. VoD system entropy increases with the degree of program aging. VoD systems run for 52 days until a crash occurs. By manually investigating reason of crash, it is assured to be an AOC. Entropy value of CPU utilization every day is calculated. It's apparent to see entropy values of last four days are much larger than ones of first four days nearly at all scales. Especially, entropy value of day 52 when computers ailed is different significantly from others. However raw CPU utilization at crash state seems normal which means crash cannot be detected if using this metric as an aging indicator. Therefore, it can be a potential aging indicator in this practice.

1.3 Conjecture

According to above observation, it provides a high level abstraction of properties that an ideal aging indicator should satisfy. *Monotonicity*; since program aging is a gradual deterioration process, aging indicator should also change consistently with degree of aging, namely increase or decrease monotonically. As most essential property, monotonicity provides a foundation to detect Aging Oriented Crash accurately. *Stability*; indicator is capable of tolerating noise or disturbance involved in runtime performance metrics. *Integration*; as program aging is a complex process affected by multiple factors, indicator should cover se influence from multiple data sources, which means it is integration of multiple runtime metrics.

In cloud computing most of PMs are converted to VMs [19]. With constant use of simulated machine and VMM causes program aging. As VMM is concept level between hardware and operating computers, many functions are running over it and are not boot up regularly.

2. LITERATURE SURVEY

Numerous studies have been carried out on program aging and renewal. Program aging is an old topic but it lacks research owing to which safety critical functions face program aging. However, some research on program aging is done in simulated setting.

Rivalino Matias et al. [20] conducted research on space associated program aging problems which produces aging and associated crashes. They concentrated on space leakage glitches. They conferred disadvantages of utilizing renowned computers wide and function-specific aging indicators and suggest effective results for their circumstances. Space-associated aging impacts are produced by space leakage and space disintegration issues. Space leakage is a computer program fault which is caused by improper utilization of space organization practices. Space leakage happens when a function process assigns space blockages and do not discharge them back to operating computers in course of its runtime. Researchers tried to discover space leakages both in user level and kernel level by utilizing aging indicators. Aging indicators detects errors in a computer in working state. Computers wide aging indicators provide information on sub computers constituents. They conducted experimentations with help of computers wide aging indicators free/used physical space and swap space. However these indicators indicate false signal regarding space usage. So aging free baseline are utilized to compare space usage with it for improved outcome. Function particular aging indicators give particular information about individual function process. For identifying space leakages, utilization of process resident set size (RSS) as aging indicator is suggested. Checking RSS in combination with procedure simulated size is an improved approach than utilizing only RSS which alone can't uncover right space.

Domenico Cotroneo et al. [21] concentrated on program aging phenomenon associated with integer runoffs. Integer runoffs are neglected issues in review of literature. Arithmetical aging related bugs signify problems for numerous long-run program functions, for example control of industrial computers and signal handling. It is difficult to evade and fix mathematical bugs, dearth of prominence for computer mathematical and program development languages by developers. Researchers presented some examples of integer overflow that causes aging. They highlighted about mathematical aging related bugs. Integer associated bugs happens when computers analyst put infinite mathematical integers to finite range. They examined and debated on various instances of numerical aging related bugs in MYSQL open source DBMS to provide physical world issues. But owing to lack of interest for integer runoffs problems, such particular renewal techniques were not developed or than restarting DBMS server. Program renewal techniques mitigate impact of program aging because of integer runoff, it lacks forecast about aging. So periodically sampling integer variables to approximate expected time to runoff for variables at run time and activate renewal methods in relation to estimated value. For future studies, performance appraisal and optimization of approach, to use method to or type of computers, and to include floating-point faults.

Autran Macedo et.al [22] suggested space related aging effects. Researchers explained, what means space management functions inward functions process, focus on two space issues that bring about program aging; disintegration and leakage. They described procedure of space-related program aging concentrating on actual and extensively accepted space allocator and offered a tentative study which shows by what means space break-up and leakage take place and by what method they accumulate over time so as to bring about computers aging-related crashes. For exploratory study, test lab consist of Intel Pentium Octa Core, 3GHz, 2GB RAM, operating on Linux with glibc 2.10.1.y formed 2 programs(Mfrag and Mleakage) to device test cases identified with space discontinuity and space spill. Though total free space in heap is bigger than amount asked for, another space is asked for in light of fact that stack is experiencing external space break-up. Asking for another block to OS infers ingoing in kernel mode, which presents an additional overhead which punishes procedure performance. Space leakage inside OS kernel influences whole computers and not a particular process, whose impacts stay until operating computers restart/reboot. In future studies, concentration is on experimenting space related impacts in simulated setting and not vulnerable to space breakup.

Lei Cui et al. [23] concentrated on in simulated setting for program aging shortcoming. Aging rate is perceived by critical experimentations on physical and VMs and recognize contrasts around two, and recommend a component code-based practice for crash foresight through computers call, then perform a model in VM official level to foresee crash time and revive. They led four experiments to recognize aging event in physical machines (PM) and VMs, and figure rate of aging for assessment. For investigation, three sorts of computers resources were gathered for measurements that demonstrate program aging Space resources; (1) Free Space and Active Space; (2) Processor resources containing User and Computers Time; (3) IO resources for instance, Block Read or Write Count and IO Waiting Time. Amid measurable examination, declining of free space size was found. Relating aging rate between PM and VM, aging rate is more prominent in VM in contrast with PM. Scholars proposed code-based strategy to expect renewal time bring up highlight models through computers calls.

Kehua Su et al. [24] proposed a work on program renewal in simulated setting (SRVE) to manage program aging marvel of VM screen and VM, and to make them enhance execution. Program running in VM computers is not boot up every now and again, so aging issues exist in VMM and VMs. So creators proposed some renewal computers for it. Methods give renewal of VMM and VMs, however it can't give zero idle time of administrations.

Kenichi Kourai et al. [25] proposed another method for quick renewal of VMM known as warm VM reboot. As VMM is basic program for running VMs, its execution debasement influences all VMs that rely upon it. So creator here proposed another program renewal procedure that recoveries both idle time cost and time. Warm-VM reboot empowers effectively rebooting a VMM by suspending and continuing VM. They created two components: on-space suspend/resume of VMs and snappy reload of a VMM. At the point when a VMM is restored by computers reboot working computers running on VMs based on top of a VMM likewise are boot up when VMM is revived. This expands idle time of managements by working computers. Here they contrasted warm VM renewal and VM movement. In this paper they clarified issue of program renewal of VMM. They executed their examination in view of Xen and performed a few experiments. They thought about various renewal strategies like computers reboot, icy VM, warm VM and VM relocation. Contrasted and an ordinary reboot, warm VM reboot decreased idle time by 75% at most. Warm VM reboot accomplished higher aggregate output than computers utilizing VM relocation and a typical reboot.

Fumio Machida et al [26] exhibited issues of ability of performance administration in a simulated information center (VDC) that has numerous administrations utilizing virtualization. Performance ability is an idea of a blended metric of execution and accessibility. Clients of a VDC demand a specific level of function execution in a service level agreement (SLA). VDC suppliers choose an ideal server design and administration operations for ensuring function execution and increasing accessibility. They concentrated on position algorithm of simulated machines and renewal plans for VMs and VMM in a VDC. VM positions, which allocate VMs to functions, are chosen for fulfilling execution prerequisites under predetermined number of physical servers. Renewal timetable are chosen for VMs and VMMs for expanding general computers accessibility in a VDC. Amid down time of a VM, number of accessible function occurrences declines and execution of function administration go down. Amid down time of a VMM, VMs and functions running on same physical server are down too. Objective of performance ability administration in a VDC is to find an ideal VM arrangement with ideal renewal plans for VMs and VMMs. ideal VM position and timetables enhance general accessibility and execution of VDC under restraints of execution levels of functions determined in SLAs.

Kenichi Kourai et al. [27] proposed another procedure for quick renewal for VMM called as warm VM reboot. When a VMM is restored working computers running on VMs based on top of a VMM additionally are boot up. This expands idle time of administrations contributed by working computers. It requires long investment to reboot numerous working computers in parallel when VMM is boot up.

Aye Myat Paing et al. [29] concentrated on renewal of VMMs effectively without influencing VMs. They joined renewal procedures with Live VM movement innovation for better advancement of resources utilization. By utilization of stochastic Petri nets they gave a model utilizing time based renewal for VMM. To assess model they gave numerical examination.

Thandar et al. [30] introduced a Markov model for investigating accessibility for long running functions which experience the ill effects of program aging. In that model they demonstrated accessibility, idle time and idle time budget amid renewal.

3. PROGRAM AGING CONCEPT

Program aging is not a new phenomenon but it was existing years before and suffering the systems and services. The concept was highlighted in year 1994 [10] after that several research studies have been undertaken to explore the issues, domain and develop corresponding solutions as for servers, applications, services and virtual machines.

3.1 Causes of Program Aging

There are two, entirely unmistakable, sorts of program aging. Initially, is brought about by crash of item's owners to adjust it to address evolving issues; second is consequence of changes that are made. This "one-two punch" prompts fast decrease in estimation of a program item.

3.1.1 Lack of development

Over three decades, assumptions about program have changed significantly. When interactive programming introduced, mysterious charge dialects were utilized. Nowadays, everybody tackles line access, "moment" reaction, and menu-driven interfaces conceded. Program is old despite the fact that no one has touched it. Clients in mid-60 were energetic about item, today's clients expect more. Unless program is often redesigned, it's client's will get to be disappointed and they will change to another item when advantages exceed expenses of retraining and changing over. They will allude to that program as old and obsolete.

3.1.2 Lack of change

Despite the fact that it is crucial to redesign program to anticipate aging, changing program causes an alternate type of aging. Program designer had a straightforward idea when composing. Program is big, understanding that idea permits one to discover those segments of project, which are modified when an update or redress is required. Understanding that idea infers understanding interfaces utilized inside and amongst computers and its surroundings. Changes are made by individuals who don't comprehend unique configuration idea quite often cause structure of computers to corrupt. Under those circumstances, changes will be conflicting with unique idea; indeed, they will discredit unique idea. Often harm is less, but sometimes it is very serious. After those developments, one must know both unique configuration rules, and recently acquainted exemptions with principles, to comprehend item. After numerous such changes, unique planners no more comprehend item. Individual who rolled out improvements, never did. At the end, no one comprehends adjusted items. Changes take longer and will probably present new "bugs". Change incited aging is frequently exacerbated by the certainty, maintainers feel they don't have sufficient time to redesign documentation. Documentation turns out to be progressively incorrect in this manner rolling out future improvements much more troublesome.

3.1.3 Lack of space allocation

Aging is computers delay brought about by crash to discharge dispensed space. Documents develop and require pruning. At time space distribution routine do not discharge all space that is assigned. Gradually, swap and document space are reduced and execution corrupts. This issue is frequently a configuration crash and is aftereffect of absence of progress or worsened by changing use designs. A clean up procedure mediates and clean up record computers and space, enhanced schedules make clean up happen quickly and computer program is considered totally "cured".

4. AGING IMPACT ANALYSIS

Examination of aging impacts (i.e., sort of invalid states brought on by aging) and aging markers in this area demonstrates how aging is showing difficulty in program computers. Aging markers are a critical zone of study, since they are instrumental for identifying when computers state is inclined to aging crashes, by observing them amid computers execution. Aging markers are pointers of resources utilization and execution markers.

Space utilization: Empirical confirmation demonstrated free space shows most brief Time to Exhaustion (TTE) among computers resources [31], and space administration faults are a noteworthy reason for crashes [32]. Therefore, numerous studies on aging and renewal analyses program aging phenomena influencing free space, by measuring quantity of free physical space and swap space [33], and a few estimation based methodologies apply time arrangement and measurable models to these variables.

Execution debasement: SAR reported execution corruption in program computers influenced by aging. A reason for execution corruption is exhaustion of computers resources: for example, utilization of physical space builds time required by space distribution methods and waste gathering instruments, since their computational intricacy is an element of measure of space regions that apportioned [34] [35]. An expanding demand reaction time and a diminishing output accounted for web functions, web servers [2], and CORBA-based functions [36]. Renewal are activated when nature of administration (e.g., as far as reaction time or throughput) is underneath a given edge.

Resources utilization: Program aging effects few sort of resources. Other than space-related resources (e.g., physical space, simulated space, swap space, cache space), studied papers manage these kinds of resources:

- File computers-related resources, for example, stream descriptors and record handles [31] [37] [38];
- Capacity, whose space is consumed by awful administration [39];
- Computers related resources, for example, attachment descriptors [37] ;
- Concurrency related resources, for example, bolts, strings and procedures [31] [38];
- Function particular resources, for example, DBMS shared pool locks [40] and OSGi references [41].

In a few studies, methodology proposed is not constrained to a particular resource, but concentrated on distinguishing inaccurate API use and wrong exemption handlers which bring about a resources spillage. Working example, [38] presents a methodology which mines resources utilization designs by checking API calls, and gives an exploratory assessment on open source programs in light of Java I/O and concurrent APIs. A normal sort of resources spillage in Java projects is characterized by outlets and record handles, because of defective exemption handlers that don't discharge these resources [37] [38]. Resources likewise are influenced by program aging depending on sort of computers, for example, free disk space in DBMS computers [39]. Some works investigate a more extensive arrangement of resources. In [31], a system of UNIX workstations was checked to distinguish aging patterns in utilization of a few resources (identified with simulated space, OS portion, file computers, disk, and organize), and critical aging pattern was seen in procedure table size and in document table size (despite the fact that their TTE is lower than TTE of free space).

Anyhow aging impacts mentioned above, re-exist other sort of aging impacts focused in late works. A field in which program renewal is studied is identified with security assaults, that is, presence of pernicious clients to access unapproved resources or to make computers inaccessible. Security assaults occur and continuously trade off a computers over a drawn out stretch of time (e.g., PIN phishing through brute force speculating, or flood assaults which trigger program aging wonders), which are lessened by intermittently reviving a computers, for example, by changing cryptographic keys, by restarting negotiated procedures, and by randomizing area of information and guidelines in space [1] [42] [43] [44] [45] [46]. A challenge in sending program renewal for security reasons for existing is to characterize exact aging pointers which are identified with security assaults. At present, aging rate are accepted at outline time [42] [47] or have to be founded on flawed assault/interference indicators which could raise false cautions and miss assaults [48] [49].

Another sort of aging impacts examined in a couple of recent works, which are alluded as other aging impacts, are identified with amassing of numerical faults [2] and space discontinuity [50] [51]. These sort of aging impacts are not inexorably brought about by bugs in program, but rather are identified with nature of floating-point mathematics and space allotment calculations, separately. An occurrence of numerical mistakes, such things in writing aging markers ready to gauge degree of faults in computers state were not found.

Finally, numerous studies propose models and methodologies for managing aging paying little attention to which particular sort of resource exhaustion or aging impact is experienced, which is normally instance of model-based studies.

The greater part of past studies concentrated on program aging impacts are identified with space utilization [31], [52], [53], performance corruption [54], [55] or both [2], [36], [34], [52]. These two perspectives are most regular issues happening in non-safety-critical computers and they are considered by an expanding number of SAR studies. These issues are less persistent for safety-critical systems. For example, an occurrence of program which experiences a safety confirmation process, dynamic space administration is avoided to achieve stringent safety integrity levels. In contrast, none of investigated research handled math issues, for example, collection of round-off faults. These faults are more applicable in safety-critical settings, with the fact that computer program is in charge of controlling physical actuators and mistaken outputs have extreme results. A surely understood case of aging crash identified with numerical faults happened in patriot rocket computers, which was created by a round-off mistake in change of aggregate execution time from a whole number to a floating-point number [33].

5. CONSEQUENCES OF PROGRAM AGING

Indications of program aging reflect those of human aging: (1) proprietors of aging program discover it difficult to stay up with business sector and lose clients to more up to date items, (2) aging program debases in its space/time execution as an after effect of slow collapsing structure, (3) aging program frequently gets to be "buggy" on account of faults presented when changes are made. Each of these results are expensive to proprietor.

5.1 Crash

As programs get aged, it becomes greater risk for crash. This "weight increase" is an aftereffect that an easy approach include an element, includes new code. Adjusting existing code to handle new circumstances is troublesome in light of the fact that code is neither surely understood nor well documented. At first, there is more code to change, a change that is made in a couple parts of unique project, now requires alternate many segments of code. Second, it is hard to discover schedules that are changed. Subsequently, proprietors can't include new components quickly. Clients change to a more youthful item to get those components. Organization encounters an eminent drop in income; when they draw out another version, it is important to a decreasing client base. They endeavor to stay aware of business sector, by expanding their work power, expanded expenses of changes, and delays, leads to further loss of clients.

5.2 Decreased Performance

As size of project develops, it puts more stress on PC space, and more defers as code are swapped in from mass storage. Program reacts slowly; clients must upgrade their PCs to get good response. Performance likewise diminishes as a result of poor configuration. Program is no more useful and changes unfavorably influence execution. The new items, whose unique configuration reflected requirement for newly presented elements will run quicker or utilize less space.

5.3 Declining Consistency

As program is kept up, mistakes are inevitable. In early years of industry, eyewitnesses record circumstances in which every mistake adjusted presented (all things considered) more than one fault. Every time an endeavor was made to reduce crash rate of computers, it deteriorated. Only decision was to forsake item or quit repairing bugs.

6. CLOUD SERIVCES AND CRASH

Principle thought behind cloud computing is highlighted in 1960, John McCarthy envisioned, general people would get computing services like a utility. Term "cloud" is utilized in many milieus, e.g., in 1990, delineating broad ATM networks. Later Google's CEO Eric Schmidt utilized word to portray business model for enabling services across over Internet in 2006, which began to pick up popularity. The term cloud computing is utilized for most part as a marketing term in various situations depict extensive thoughts. But lack of standard meaning of cloud computing has created market build-ups, as well as lot of doubt and perplexity. Consequently, as of late there are work on institutionalizing meaning of cloud computing. As an illustration, work in looked at more than 20 unique definitions from an assortment of sources to affirm a standard definition. This study embrace meaning of cloud computing gave by National Institute of Standards and Technology (NIST) [56].

NIST meaning of cloud computing "Cloud computing is a model for empowering advantageous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storages, functions, and services) which are quickly provisioned and discharged with negligible management effort or service provider interaction."

Principle purpose behind presence of various impression of cloud computing is that cloud computing is quite an old technology, yet rather a new operations model which unites present technologies to run business in an unexpected way. The vast majority of advances utilized by cloud computing, for example, virtualization and utility-based estimation, are not new. Rather, cloud computing influences these existing innovations to meet mechanical and economic necessities of today's demand for IT.

Cloud service failure can happen once or frequently. There causes for it but aging of program are also one of them, which is propagated with the program bugs. When disaster does strike, there’s no physical data center you can visit to investigate the problem. Below are given some reasons for cloud service crash [63].

6.1 Cloud Provider Downtime

This is because of service provider who provides the cloud infrastructure management and hosting service. It the proper back is done and distributed computing in adopted then risk can be reduced and prevent downtime.

6.2 Security Attacks

If security requirements and concerns are not taking in advance attention than most probably system can be weak and major risk to attack.

6.3 Storage Failures

This can be a top level risk to cloud service crash and system down. Storage failure is serious cause of service crash and unavailability.

6.4 Human Error

This is the mal practice done by the professional who manage the cloud application and service manager. Level of expertise and experience must be as good as possible.

6.5 Demand fluctuation

Sometimes the demand of cloud service are more sometime less. In this type of situation it is managed by system to extend and shrink the infrastructural context to manage the increased and decreased demand of service.

6.6 Third Party Service Failures

The incorporated application and services provided by the third party have to be continuously monitor to proper function of cloud service. Many times the third party application are down on which the current service depends also crash.

6.7 Quality of Service

Poor quality if service , which may have many parameters like network, speed of response, system performance , quality of streaming etc. can also affect the operation the cloud service.

6.8 Poor crash recovery procedures

Every cloud based organizations have to manage the strong recovery system procedure for service crash. The application should include the recovery mechanism and procedure for effective and timely practice.

6.9 Application Bugs

There can be certain types of bugs found in application at run time or even at deployment time which can lead to a service crash and system failure.

7. PERFORMANCE ANALYSIS OF SERVICE DEGRADATION

A significant consideration is dedicated to empirical investigation of program aging from original computers. Since, marvel shows itself as performance corruption and/or resources utilization specialists concentrated on methodologies for extracting estimations from computers [1].

To evaluate job load of computers, number of jobs succumbed to computers every day, on the basis of their start time is considered. To measure performance, normal length of jobs every day, that is, by calculating mean estimation of term of jobs finished every day, on basis of their completion time and submission time. Irrespective of the fact that these measurements give a halfway sign of job load and of performance, these measurements are effectively figured from dataset that was accessible, and empower a preparatory examination of performance debasements.

Study of performance of computers in general (i.e., without part information by node/line and by utilization period) did not point out any diminishing patterns of performance. Rather, some performance debasement patterns on a little subset of nodes and lines in supercomputer was discovered. This recommends program aging wonders are limited in a particular piece of computers for particular sorts of job load. Assumption is generated because of (i) program aging problems (e.g., resources leakages) that are present in program of influenced nodes or lines, and/or (ii) particular sorts of jobs which generate these problems. The investigation on nodes displayed a performance debasement pattern (i.e., a huge increment in normal span of jobs).

Granger causality test pointed out that these performance debasement patterns appear not to be identified with variations in job load. This outcome gives some certainty that patterns are not identified with random varieties of job load, and it is worth to investigate these drifts more carefully. If the normal job accomplishment time is expanding, job load showed comparable varieties, in this manner providing reason to feel ambiguous about presence of a program aging marvel behind that performance pattern.

8. PARAMETERS OF SERVICES PERFORMANCE DECLINATION

More extensive scope of cloud service, which related to programs, gets ineffective. Aside from security issues, for example, securing innumerable bits of individual information scattered in cloud or conceivable protection infringement, countermeasure arrangements are set up to control computer program weakness. An issue suffered by one occupant raise to another occupant in the event that they share same service. Overcoming dangers connected to vulnerabilities and giving more dependable, higher quality service than contenders are greatest achievement component. Program weakness has not been altogether taken care of in best practices for conventional program improvement yet, so technology is not developing enough to manage shortcomings in cloud service. Weakness control of cloud service requires comparing counter measures for anticipated weakness issues when scope of service clients is not constrained.

It gives information and markers of performance, where that performance level influences reception of cloud services by clients. Performance is among points of interest that ought to be accessible in cloud services since performance affects clients and service providers. To assess performance, consider a few criteria to assess components that influence performance of cloud services, including normal reaction per unit time and normal holding up time per unit time and others in properties of performance measures of cloud [57].

- SaaS - Evaluation is made by clients specifically relying upon performance measures, velocity of reaction, dependability of specialized services and accessibility.

- Pass - Evaluation is made by clients specifically or by implication relying upon performance measures in light of detail, efficiency, dependability, specialized service and middleware capacity.

- IaSS - Performance measures are resolved relying upon framework performance, limit, unwavering quality, accessibility, and versatility.

Performance and assessment are measured relying upon responsive time, efficiency, and timing in executing jobs, viz., and handling activities in suitable period. The SLA, agreement confines clients and cloud service providers. Levels of service or quality of service (QOS) are considered. Service performance is portrayed by reaction time, profitability, accessibility, and security. Quality of Service (QoS) in cloud shows level of performance and dependability, regardless of the fact that attributes of quality of service got consideration before development of cloud, performance, homogeneity as well as principles [58].

To perform an operation at which capacity and security are accomplished, viz., any service ability to guarantee classification of a bit of information worked with, traded or put away, confidentiality of correspondences, legitimacy and safety of traded or put away information, and protection of client and his correspondence implies against any sort of danger, notwithstanding or characteristics of exactness, unwavering quality, adaptability and convenience [59]. There are a few dangers and confronting clients when they utilize cloud services. They are expanding, that when service providers or resources exist outside local extension, viz., they are under various laws. In connection to appropriation of cloud in advanced education, there are some difficulties, for example, security, performance, proficiency and control [31].

Security element influence performance through security sway on network framework, for instance, is case with DDoS assaults which broadly affect network performance. This danger or any dangers that undermine cloud environment, it will be a noteworthy matter for clients and suppliers [60]. These assaults are hurtful to computing. Protecting SQL assault permits assailant access to database. Likewise, in flood assaults assailant sends a solicitation for resources to cloud so rapidly that he exploits capacity of any remote resources by normal clients and here numerous assaults which incapacitate security of cloud happen [61]. Security is a vital need to cloud clients. Decision is to make utilization of cloud services founded on level of secrecy, honesty, adaptability, and security services accessible, and this is a sign to rivalry among service providers which prompts advancement of cloud computing [30]. There are a few issues confronting cloud computing clients, as far as access to information through Internet; any shortcoming in level of security in cloud is debilitating secrecy of clients information stored. In addition, quality of association influences level of performance in conveyance of services, high cost of private automated computing contrasted and open and blended segments, at cost of quality, performance and security [40].

9. RELATIONSHIP OF SERVICE PERFORMANCE WITH AGING PARAMETER

When computing resources almost depleted, variety of resources variable will bring about or resources variables to change. Three imperative resources variables change clearly. An inquiry is the way to recognize which resources variable is main driver of harming steadiness of resources dissemination of PC. The underlying driver of program aging is buffer expand, unmoved CPU reduction and cache diminish separate in three times of simulation, and test where output of the model fit perceptions.

Particularly, input of real estimation of one parameter and starting estimation of or two parameters into model, and figure estimation of or two parameters with time. For instance, the real estimation of buffer and introductory estimations of inactive CPU and cache as input parameters. The inactive CPU and cache of dynamic model is figured out at next interim by repeat, with real estimation of buffer as input value. Further, the cache or inactive CPU as input parameters individually and ascertain other two parameters. Results are not recorded on the grounds that output of element model can't fit observations.

Buffer use increment causes change of other parameters, will output comparable dynamics as exploratory perceptions. There are a few reasons: (1) this model utilizes three variables, so bond between three variables is not precisely depicted; (2) buffer utilization increment is the reason of other two variables, numerous auxiliary elements are excluded in this model; (3) More higher request of polynomials will bring higher exactness, while utilizing quadratic polynomials. In spite of substantial mistakes, this model is compelling, on the grounds that the item in simulation is to investigate which resources variable is underlying driver of program aging, rather than precisely gauging estimation of cache or accessible CPU. This examination helps to comprehend conduct of computer program when it slowly ages.

10. RESULTS AND DISCUSSIONS

To distinguish a relationship amongst measurements and aging, the initial step is to assess connection with individual measurements. Pearson connection coefficient between every metric and aging patterns were evaluated; this coefficient are utilized to test a direct connection between two variables [1]. Measurements with a measurably noteworthy relationship (p-esteem < 0:05) are observed. All measurements identified with computers size are connected with program aging. This affirms assumption that there occurs an association between program aging and program multifaceted nature. Few measurements don't show direct connection with numerical implications. It is included in resulting investigation; there is a non-linear relationship (alone or in blend with or measurements) not found by this preparatory test.

Statistical regression models were adopted to acquire a quantitative relationship between program measurements and aging. Since a direct relationship with a few measurements was watched, various straight relapse models were assessed. To make this model, common relationship among measurements, e.g., a program with high LOC will have a high number of capacity affirmations, needs to be managed; this connection prompts an instable model, since little change in information bring about expansive change in model. Therefore, stepwise strategy to manufacture model, viz., particular variables are presented or expelled from model and a statistical significance test is performed to choose top model. This technique created a linear model with one variable.

The model is described by high standard deviation of residuals (1:3185 MB/h). This high fluctuation influences expectation for program modules with a low aging pattern (1 MB/h), prompting a high normal relative mistake (1:686 106%). In addition, free variables are portrayed by a high inter correlation, since one variable is brought into model by stepwise technique.

To get an exact model, Principal Component Analysis (PCA) strategy was adopted, which changes dependant variables in a small number of uncorrelated variables [62]; yet, this methodology did not enhance model. An exponential and a logarithmic model was assessed, however they were not ready to give better accuracy. Absence of basic and exact model is because of heterogeneity of program modules. A perceptible element of dataset is expansive scope of qualities in aging patterns, they vary by a few order of magnitude. Therefore, dataset was isolated into two disjoint clusters, in particular Big Aging and Little Aging, which were exclusively broke down. Two gatherings were considered because of low number of program modules. Subsequently breaking dataset, stepwise technique to gatherings was connected. Substantially exact model in both cases were acquired. Both models fulfil hypotheses of residuals' homoscedasticity, typicality, and un-correlation with autonomous variables. Specifically, model for little aging gathering is portrayed by a low standard deviation and a satisfactory normal relative fault (around 11%). Dependant variables incorporated into this model, Ratio Comment To Code and Count Line Inactive, don't have all the representative of program complexity; nonetheless, given high relationship between dependant variables, it is inferred that aging pattern of program of this gathering is identified with project size, both dependant variables have a place with this sort of measurements. Although model for Big Aging gathering is superior to opening model, it is described by a high mistake. It is suspected that mistake was because of presence of trace module in gathering, since it is described by a low intricacy and high aging patterns. Therefore, this example is an anomaly and expelled it from gathering;

resultant model was much more precise, with a low normal relative error, around 8%. This outcome was because of immaturity of trace module, which was influenced by extreme aging-related bugs irrespective of the fact that it was a moderately basic module. In this gathering, aging is identified with size of modules (LOC); model represents complex quality of code (Volume). At last, to clarify contrast between two gatherings, and to apply right model to another program, i.e., excluded in dataset, it was assessed on the possibility to characterized modules into gatherings utilizing program measurements. To choose best components, i.e., measurements, to use in classifier, feature choice computers was applied, in particular independent features methodology [62]. This technique performs a statistical test for each individual component, showing that distinction is unrealistic to be random variation; if contrast is sig times lower than standard mistake, then highlight is not regarded valuable for ordering. The test is performed by assessing

$$se\ (A\text{-}B)=\sqrt{\frac{var\ (A)}{nA}+\frac{var\ (B)}{nB}} \qquad (1)$$

$$\frac{|mean\ (A)-mean\ (B)|}{se\ (A-B)} > sig \qquad (2)$$

Where A and B are same component measured for two divisions, and nA and nB number of samples in classes. Many components were considered utilizing diverse estimations of sig. Adequacy of every arrangement of components utilizing leave- one out strategy: n-1 samples are utilized for preparing a classifier, and rest of the example is utilized for testing classifier; the rest of the samples are utilized for various splitting of dataset. For classification, two-class SVM classifiers were adopted.

Table 1 shows results of put one out validation of best classifier (sig = 3:4). This classifier is effective in 9 out of 10 cases; it is not exact in the event of trace module, which was beforehand appeared to be an irregular example. Feature choice and leave one out authentications were revised without trace service, and best classifier accurately characterized samples in all cases. This outcome bolsters utilization of program measurements for characterizing program regarding aging. Measurements of best classifier were Volume (mean), Effort (mean), Volume (difference), N1 (change), N2 (fluctuation), Length (change).

Table 1: Leave-one-out validation (LA = Little Aging, BA = Big Aging) for sig = 3:4.

Module	Reference class	Anticipated class
Garbage collector	BA	BA
JIT Compiler	BA	BA
Trace	BA	LA
Common	LA	LA
Repository	LA	LA
Load balancing	LA	LA
Xerces	LA	LA
Httpd	BA	BA

11. CONCLUSION

Relationship between program measurements and program aging on ten computer program functions were researched. Program functions belong to two particular gatherings, in which aging impacts are insignificant (Little Aging), and program fundamentally influenced by program aging (Big Aging). A basic model ready to foresee aging impacts of both gatherings at same time were not found, in this manner they are broke down independently. There exist two exact multiple linear regression models for modeling two programs function clusters. Aging patterns in Little Aging group appears to be connected with program size, while difficulty of project as far as operands and administrators, i.e., Halstead measurements, are considered for Big Aging groups. It is probable to arrange program functions in one of two gatherings by utilizing program measurements. Halstead measurements ended up being most appropriate for this reason. These results empower utilization of program measurements for adapting to program aging at advancement time. The classification, of another program is made by recognizing its class (Little Aging or Big Aging), and then applying a customized linear regression model.

Clouds have developed as a definite worldview for managing and assigning services over network. Rise of cloud computing is rapidly shifting prospect of IT, and altering long-held assurance of utility computing into a reality. In spite of noteworthy advantages offered by cloud computing, current advancements are not sufficiently developed to understand its maximum capacity. Many problems in this field, counting programmed resources provisioning, power administration and safety administration, are getting consideration from examination group. There is still enormous opportunity for analysts to make noteworthy contributions in this field, and convey huge effect to their advancement in industry. Examination of aging impacts and aging pointers reports that space and performance issues were most studied in literature.

In this paper, condition of specialty of cloud service performance degradation have been highlighted based on one parameter of program aging among various other parameters and specific causes. The study have shown that a significantly aged program is a high risk and performance failure, can lead to permanent crash of services. Program renewal and SAR have been identified some level of solution approaches but still under investigation and further research to find out a suitable solution of Aging Oriented Crash.

12. REFERENCES

[1] Huang, Y., Kintala, C., Kolettis, N., and Fulton, N. 1995. Computer program renewal: analysis, module and functions. In Fault-Tolerant Computing, 1995. FTCS-25. Digest of Papers, Twenty-Fifth Int'l. Symp.

[2] Grottke, M., Matias, R., and Trivedi, K. 2008. The fundamentals of computer program aging. In Computer program Reliability Engineering Workshops, 2008. IEEE

Int'l. Conf.

[3] Bernstein, L. and Kintala, C. 2004. Computer program renewal. CrossTalk 17, 8, 23–26.

[4] Avritzer, A. and Weyuker, E. 1997. Monitoring smoothly degrading computerss for increased dependability. Empirical Computer program Engineering 2, 1, 59–77.

[5] Marshall, E. 1992. Fatal error: how patriot overlooked a scud. Science 255, 5050, 1347–1347.

[6] Bernstein, L. 1993. Innovative technologies for preventing network outages. AT & T TECH J. 72, 4, 4–10.

[7] Wang, Y.M., Huang, Y., Vo, K.P., Chung, P.Y., and Kintala, C. 1995. Checkpointing and its functions In Fault-Tolerant Computing, 1995. FTCS-25. Digest of Papers., Twenty-Fifth Int'l. Symp.

[8] Kajko Mattsson, M. 2001. Can we learn anything from hardware preventive maintenance? In Engineering of Complex Computer Computerss, 2001. Proceedings. Seventh IEEE International Conference on. IEEE, 106–111.

[9] Adams, E. 1984. Optimizing preventive service of computer program products. IBM Journal of Research and Development 28, 1, 2–14.

[10] Parnas, D. 1994. Computer program aging. In Proceedings of the 16th international conference on Computer program engineering. IEEE Computer Society Press, 279–287.

[11] K. Vaidyanathan and K. S. Trivedi, "A measurement-based model for estimation of resource exhaustion in operational computer program computerss," in Computer program Reliability Engineering, 1999. Proceedings. 10th International Symposium on. IEEE, 1999, pp. 84–93.

[12] K. Vaidyanathan, R. E. Harper, S. W. Hunter, and K. S. Trivedi "Analysis and implementation of computer program renewal in cluster computerss," in ACM SIGMETRICS Performance Evaluation Review, vol. 29, no. 1. ACM, 2001, pp. 62–71.

[13] M. Grottke, L. Li, K. Vaidyanathan, and K. S. Trivedi, "Analysis of computer program aging in a web server," Reliability, IEEE Transactions on vol. 55, no. 3, pp. 411–420, 2006.

[14] J. Alonso, J. Torres, J. L. Berral, and R. Gavalda, "Adaptive online computer program aging prediction based on machine learning," in Dependable Conference on. IEEE, 2010, pp. 507–516.

[15] Y. F. Jia, L. Zhao, and K.Y. Cai, "A nonlinear approach to modeling of computer program aging in a web server," in Computer program Engineering Conference, 2008. APSEC'08. 15th Asia-Pacific. IEEE, 2008, pp. 77–84.

[16] P. Zheng, Y. Qi, Y. Zhou, P. Chen, J. Zhan, and M. Lyu, "An automatic framework for detecting and characterizing performance degradation of computer program computerss," Reliability, IEEE Transactions on, vol. 63, no. 4, pp. 927–943, 2014.

[17] S. Garg, A. van Moorsel, K. Vaidyanathan, and K. S. Trivedi, "A methodology for detection and estimation of computer program aging," in Computer program Reliability Engineering, 1998. Proceedings. The Ninth International Symposium on. IEEE, 1998, pp. 283–292.

[18] M. Shereshevsky, J. Crowell, B. Cukic, V. Gandikota, and Y. Liu "Computer program aging and multifractality of space resources," in 2003 33rd Annual IEEE/IFIP International Conference on Dependable Computerss and Networks (DSN). IEEE Computer Society, 2003, pp.721.

[19] J. Araujo, R. Matos, P. Maciel, R. Matias, and I. Beicker, "Experimental evaluation of computer program aging effects on the eucalyptus cloud computing infrastructure," in Proceedings of the Middleware 2011 Industry Track Workshop. ACM, 2011, p. 4.

[20] Rivalino Matias Jr., Bruno Evangelista Costa, and Autran Macedo, "Monitoring Space-Related Computer program Aging: An Exploratory Study" ,IEEE, 2012.

[21] Vols. Domenico Cotroneo, and Roberto Natella, Monitoring of Aging Computer program Computerss affected by Integer Overflows, IEEE, 2012.

[22] Autran Macêdo, Taís B. Ferreira, and Rivalino Matias Jr, "The Mechanics of Space-Related Computer program Aging," IEEE ,2011.

[23] Lei Cui, Bo Li, Jianxin Li, James Hardy, and Lu Liu, "Computer program Aging in Simulated Environments: Detection and Prediction," IEEE, 2012.

[24] Kehua Su, Hongbo Fu, Jie Li, and Dengyi Zhang, "Computer program Renewal in Virtualization Environment," IEEE, 2011.

[25] Kenichi Kourai, and Shigeru Chiba, "Fast Computer program Renewal of Simulated Machine Monitors," IEEE, Vol 8, No 6, 2011.

[26] Fumio Machida, Dong Seong Kim, Jong Sou Park, and Kishor S. Trivedi, " Toward Optimal Simulated Machine Placement and Renewal Scheduling in a Simulated Data Center," IEEE, 2008.

[27] Kenichi Kourai, and Shigeru Chiba, "A Fast Renewal Technique for Server Consolidation with Simulated Machines, " IEEE, 2007.

[28] Fumio Machida, Jianwen Xiang, Kumiko Tadano, and

Yoshiharu Maeno, "Combined Server Renewal in a Simulated Data Center.

[29] Aye Myat Myat Paing, and Ni Lar Thein, " High Availability Solution: Resource Usage Management In Simulated Computer program Aging, Aye Myat Myat Paing, and Ni Lar Thein, " High Availability Solution: Resource Usage Management In Simulated Computer program Aging.

[30] Thandar Thein, Sung-Do Chi, and Jong Sou Park," Availability Analysis and Improvement of Computer program Renewal Using Virtualization," Economics and Applied Informatics, Years XIII, 2007.

[31] Garg, S., Van Moorsel, A., Vaidyanathan, K., and Trivedi, K. 1998b. A methodology for detection and estimation of computer program aging. In Computer program Reliability Engineering, 1998. Proc. Ninth Int'l. Symp.

[32] Sullivan, M. and Chillarege, R. 1991. Computer program Defects and Their Impact on Computers Availability—A Study of Field Crashs in Operating Computerss. In Fault-Tolerant Computing, 1991. FTCS-21. Digest of Papers., Twenty-First International Symposium. IEEE, 2–9.

[33] Grottke, M., Li, L., Vaidyanathan, K., and Trivedi, K. 2006. Analysis of computer program aging in a web server. Reliability, IEEE Transactions on 55, 3.

[34] Carrozza, G., Cotroneo, D., Natella, R., Pecchia, A., and Russo, S. 2010. Space leak analysis of mission-critical middleware. Journal of Computerss and Computer program 83, 9, 1556–1567.

[35] Cotroneo, D., Orlando, S., Pietrantuono, R., and Russo, S. 2011b. A measurement-based ageing analysis of the jvm. Computer program Testing Verification and Reliability.

[36] Cotroneo, D., Natella, R., Pietrantuono, R., and Russo, S. 2010. Computer program aging analysis of the linux operating computers. In Computer program Reliability Engineering (ISSRE), 2010 IEEE 21st Int'l. Symp.

[37] Weimer, W. 2006. Exception-handling bugs in java and a language extension to avoid them. Lecture Notes in Computer Science 4119 LNCS, 22–41.

[38] Zhang, H., Wu, G., Chow, K., Yu, Z., and Xing, X. 2011. Detecting resource leaks through dynamica mining of resource usage patterns. In Dependable Computerss and Networks Workshops (DSN-W), 2011 41st Int'l. Conf.

[39] Bobbio, A. and Sereno, M. 1998. Fine grained computer program renewal models. In Computer Performance and Dependability Symposium, 1998. IPDS'98. Proceedings. IEEE International. IEEE, 4–12.

[40] Cassidy, K., Gross, K., and Malekpour, A. 2002. Advanced pattern recognition for detection of complex and Networks, 2002. Proc. Int'l. Conf.

[41] Gama, K. and Donsez, D. 2008. Service coroner: A diagnostic tool for locating osgi stale references. EUROMICRO 2008 - Proceedings of the 34th EUROMICRO Conference on Computer program Engineering and Advanced Functions, SEAA 2008, 108–115.

[42] Sousa, P., Bessani, A., Correia, M., Neves, N., and Verissimo, P. 2010. Highly available intrusion tolerant on 21, 4, 452 –465.

[43] Tai, A., Tso, K., Sanders, W., and Chau, S. 2005. A performability-oriented computer program renewal framework for distributed functions. In Dependable Computerss and Networks, 2005. Proc. Int'l. Conf.

[44] Valdes, A., Almgren, M., Cheung, S., Deswarte, Y., Dutertre, B., Levy, J., Saidi, H., Stavridou V., and Uribe, T. 2003. An architecture for an adaptive intrusion-tolerant server. Lecture Notes in Computer Science (including subseries Lecture Notes.

[45] Cox , B., Evans, D., Filipi, A., Rowanhill, J., Hu, W., Davidson, J., Knight, J., Nguyen-Tuong,A., and Hiser, J. 2006. N-variant computerss: a secretless framework for security through diversity. In Proceedings of the 15th conference on USENIX Security.

[46] Roeder, T. and Schneider, F. 2010. Proactive obfuscation. ACM Transactions on Computer Computerss (TOCS) 28, 2, 4.

[47] Nguyen, Q. and Sood, A. 2009. Quantitative approach to tuning of a time-based intrusion-tolerant computers architecture. In Proc. 3rd Workshop Recent Advances on Intrusion-Tolerant Computerss. 132–139.

[48] Aung, K., Park, K., and Park, J. 2005. A model of its using cold standby cluster. Lecture Notes in Computer AUNG, K., PARK, K., AND PARK, J. 2005. A model of its using cold standby cluster. Lecture Notes in Computer Science 3815 LNCS, 1–10.

[49] Nagarajan, A. and Sood A., "SCIT and IDS architectures for reduced data ex-filtration", DSNW, 2010, Dependable Systems and Networks Workshops, Dependable Systems and Networks Workshops 2010, pp. 164-169, doi:10.1109/DSNW.2010.5542601.

[50] Grottke, M., Matias, R., and Trivedi, K. 2008. The fundamentals of computer program aging. In Computer program Reliability Engineering Workshops, 2008. IEEE Int'l. Conf.

[51] Macedo, A., Ferreira, T., and Matias, R. 2010. The mechanics of space-related computer program aging. In

Computer program Aging and Renewal (WoSAR), 2010 IEEE Second Int’l. Workshop on.

[52] Matias, R., Barbetta, P., Trivedi, K., and Filho, P. 2010a. Accelerated degradation tests applied to computer program aging experimentations. Reliability, IEEE Transactions on 59, 1.

[53] Shereshevsky, M., Crowell, J., Cukic, B., Gandikota, V., and Liu, Y. 2003. Computer program aging and multifractality of space resources. In Dependable Computerss and Networks, 2003. Proc. 2003 Int’l. Conf.

[54] Magalhaes, J. and Silva, L. 2010. Prediction of performance anomalies in web-functions based-on computer program aging scenarios. In Computer program Aging and Renewal (WoSAR), 2010 IEEE Second Int’l. Workshop on.

[55] Zhao, J. and Trivedi, K. 2011. Performance modeling of apache web server affected by aging. In Computer program Aging and Renewal (WoSAR), 2011 IEEE Third International Workshop on. 56 –61.

[56] A. Andrzejak and L. Silva, “Using machine learning for non intrusive modeling and prediction of computer program aging,” in Network Operations and Management Symposium, 2008. NOMS 2008. IEEE IEEE, 2008, pp. 25–32.

[57] D. Cotroneo, R. Natella, R. Pietrantuono, and S. Russo, “Computer program aging analysis of the linux operating computers,” in Computer program Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on IEEE, 2010, pp. 71–80.

[58] B. Sharma, P. Jayachandran, A. Verma, and C. R. Das, “Cloudpd: Problem determination and diagnosis in shared dynamic clouds in IEEE DSN, 2013.

[59] P. Zheng, Y. Qi, Y. Zhou, P. Chen, J. Zhan, and M. Lyu, “An automatic framework for detecting and characterizing performance degradation of computer program computerss,” Reliability, IEEE Transactions on vol. 63, no. 4, pp. 927–943, 2014.

[60] M. U. Ahmed and D. P. Mandic, “Multivariate multiscale entropy: A tool for complexity analysis of multichannel data,” Physical Review E, vol. 84, no. 6, p. 061918, 2011.

[61] L. Cao, A. Mees, and K. Judd, “Dynamics from multivariate time series,” Physica D: Nonlinear Phenomena, vol. 121, no. 1, pp. 75–88,, 1998.

[62] J. F. Cadima and I. T. Jolliffe, “Variable selection and the interpretation of principal subspaces,” Journal of agricultural, biological, and environmental statistics, vol. 6, no. 1, pp. 62–79, 2001.

[63] http://www.eweek.com/cloud/slideshows/nine-common-reasons-cloud-systems-crash.html

International Journal of Computer Applications Technology and Research
Volume 5– Issue 7, 433 - 438, 2016, ISSN:- 2319–8656

A Lightweight Algorithm for Detecting Sybil Attack in Mobile Wireless Sensor Networks using Sink Nodes

Abdolreza Andalib
Department Of Computer Software, Qeshm International Branch, Islamic Azad University, Iran

Mojtaba Jamshidi
Department Of Computer Software, Qazvin Branch, Islamic Azad University, Iran

Farahnaz Andalib
Department Of Computer Software, Kermanshah Branch, Islamic Azad University, Iran

Davod Momeni
Department Of Computer Software, Kermanshah Branch, Islamic Azad University, Iran

Abstract: Considering the application of wireless sensor networks in critical area, such as battlefields, establishing security in these networks is of utmost importance. One of the most serious and dangerous attack against these networks is Sybil attack. In this attack, a malicious hostile node creates multiple fake identities simultaneously. This misleads legitimate nodes and, by mistake, they assume each of these identifiers as real separate nodes. In this attack, malicious hostile node attracts so heavy traffic that can dramatically disrupt routing protocols which has devastating effects on the network functions such as data integration, voting, and resource allocation. The current research proposes a new lightweight algorithm for detecting Sybil attack in Mobile Wireless Sensor Networks using sink nodes. The proposed algorithm is implemented to be assessed in terms of detection and error rates efficiency in a series of experiments. Comparison of the experiment results with the results of other available algorithms revealed optimal performance of the proposed algorithm.

Keywords: Wireless Sensor Networks, Sybil attack, Lightweight algorithm, Sink nodes

1. INTRODUCTION

A wireless sensor network consists of hundreds to thousands small and inexpensive sensor nodes that work together to provide the possibility of monitoring the environment and collecting information. In such networks, usually, there are one to several sink nodes that collect all network data and send commands to one, several or all network nodes. In other words, after capturing (or sensing) information from the environment, sensor nodes send them, step by step, to sink node(s). Being inexpensive and small, sensor nodes have limitations in terms of energy, memory, and computing capability. Because of these limitations, complex encryption and security algorithms of other networks (such as local networks) cannot be applied and set up on the “resource limited” sensor nodes. However, sink nodes do not have such limitations and are usually informed about general network data including encryption keys, number of nodes, nodes identities, etc. [1].

Sybil attack is one of the major attacks that affect the routing layer. In this attack, as indicated in figure 1, a malicious hostile node, after being distributed in the operating network environment, creates multiple fake identities simultaneously, called Sybil nodes (herein after called “Sybil nodes”). In figure 1, each normal node has only one identity while each malicious node creates 6 identities (IDs 5-10). This misleads neighboring legitimate nodes and they assume each of these Sybil nodes is a real separate node, Whereas, all the Sybil nodes are just and only a real (malicious hostile) node. Therefore, the hostile node attracts so heavy traffic and disrupts routing protocols to a large extent which has devastating effects on the network functions such as data integration, voting, and resource allocation [2][3][4].

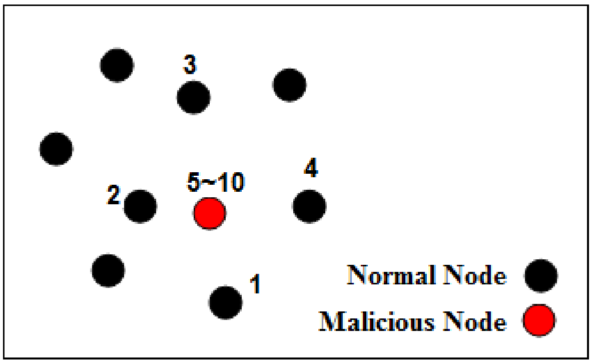


Figure 1 – An example of Sybil attack set-up

So far, various strategies are developed to counteract with Sybil attack in fixed sensor networks. In [5], for instance, an algorithm is proposed, based on radio resource testing, to detect Sybil nodes in which each node assigns a different channel to each of its neighbors to broadcast some message on. However, this method is not efficient considering the limitations of sensor nodes (assigning a separate channel to each neighbor). Also, strategies based on identity verification, such as those proposed in [5] and [6], firstly require a huge memory space and secondly get involved in processing complex checking algorithms in order to store essential identity verification data (including shared encryption keys, identity certificates, etc.). In addition, strategies based on Received Signal Strength Indicator (RSSI) [7], as the one developed in [8], cannot be proper solutions, as well, since the radio signal is susceptible to be interfered by the environment, on one hand, and the malicious node can fail the algorithm by adjusting its sending power, on the other hand. So, using these strategies for detecting Sybil nodes of mobile sensor networks will not be effective. Because, in the first place, these strategies impose heavy costs (computing, communication and memory) on resource-limited sensor nodes. Second, due to nodes mobility in mobile sensor networks, the above mentioned algorithms either have errors or fail in the process of detecting Sybil nodes.

In this paper, a new lightweight algorithm for detecting Sybil attack in Mobile Wireless Sensor Networks is proposed. The main underlying idea of the proposed algorithm is exchanging a random number between sink and sensor nodes.

The rest of this paper is organized as follows: section 2 reviews the literature. Section 3 explains system hypotheses and the attack model. Section 4 elaborates on the proposed algorithm and section 5 gives the performance evaluation and simulation results. Finally, section 6 concludes the paper.

2. Literature Review

Sybil attack was introduced in [4], for the first time, for peer-to-peer networks. Researchers in [5] analyzed the attack in wireless sensor networks, for the first time, and developed several defense mechanisms including radio resource testing, key validation for random key predistribution, position verification, identifier registration, and remote code verification or code attestation. In radio resource testing, each node assigns a separate channel to its neighbors to broadcast on. In identifier registration approach, a trusted central authority poll the network to identify Sybil nodes. In [7] an algorithm is proposed based on Received Signal Strength Indicator (RSSI) to estimate the location of nodes in the network. In [8] the locating mechanism proposed in [7] is used for detecting Sybil nodes. The algorithm uses four location-aware (routing) nodes that are capable of hearing the packages from all network areas to detect Sybil nodes. When a node sends a package, routing nodes cooperate to estimate its location. It is enough to identify the target nodes because all Sybil nodes are located in a same area. The method which is developed in [9] for detecting Sybil nodes needs no hardware or information about signal strength yet it solely uses data regarding the number of neighbors to identify malicious node and fake (Sybil) identities. The algorithm functions in a distributed manner based on no central point such as base stations or specific nodes (location-aware). Also, [10] proposed an algorithm based on Received Signal Strength Indicator (RSSI) mechanism to detect Sybil attacks in sensor networks that use Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for clustering. [11] Proposed another algorithm based on RSSI technique to detect Sybil nodes when the nodes are adjusting the broadcasting power. In [12] a new algorithm is proposed based on identifying Angle of Arrival (AOA) mechanism called Trust Evaluation Based on AOA (TEBA). Considering that a Sybil nodes can create multiple identities with only one real location, anchor nodes detects Sybil identities that their signal phase difference is less that trust threshold (calculated by assessing trust angle of neighboring sensor nodes). In [13] a method is developed to counteract with Sybil attack which collects route information by collective intelligence algorithm during network activity and detects Sybil node by its energy changes in the meantime. Also, in [14], another RSSI-based algorithm is proposed for detecting Sybil nodes in LEACH routing protocol. IN [16], a new algorithm is proposed based upon customer puzzles and learning automata to deal with Sybil attacks in wireless sensor networks. Added to these, in [17] and [18], other algorithms are proposed that uses guard nodes in detecting Sybil nodes in mobile sensor networks.

3. System Hypotheses and the Attack Model

A sensor network contains n sensor nodes and m sink nodes that are randomly distributed in a two-dimensional area. All sensor nodes are mobile and, according to mobile models (such as Random waypoint), move in the operating environment during the network lifetime. Sink nodes may be mobile or fixed, as well. Each node has one identity and is unaware of its own location. Nodes communicate via wireless radio channels and use Omni-directional distribution approach. Radio range of all nodes (sensor and sink) are the same and equal to r. It is also assumed that sensor nodes cannot resist against interference and enemies can access their confidential information in case of capturing them so as to reprogram them. But, sink nodes are equipped with tamper-resistant hardware and enemies cannot decode and reprogram them.

Here, an attack model is considered, based upon classifications given in [5], i.e. “direct, simultaneous, and stolen identities” Sybil attack. That is, the enemy captures multiple valid identities (e.g. S1~S10) in the network, first. Then, program a malicious node so that it creates S1 to S10 (Sybil nodes) identities simultaneously after being deployed in the network operating environment. In addition, legitimate nodes communicate with Sybil nodes “directly” (not through another node). It should be noted that enemy creates malicious either by itself or by capturing and reprogramming legitimate nodes in the network. Like normal sensor nodes, malicious nodes can move in the operation environment. Considering the attack model, it is assumed that our network has an identity assignment mechanism [19]. In the identity assignment mechanism, the enemy is not capable of creating fake identities; therefore, it has to capture legitimate nodes of the network to set up a Sybil attack. It is also assumed that each node has to send a “Hello” or “route request” message, by arriving at a new location in the network. In fact, this is a requirement for mobile sensor networks so each node can identify its neighbors instantly, set up a security key with them (if necessary), communicate, create its own routing table, etc. [20]. It is obvious that, in this case, each malicious node must send a “hello”, “route request”, etc. message per each of its Sybil identities, after arriving at a new location in the network (simultaneous Sybil attack [5]). Our proposed algorithm detects Sybil nodes by such kinds of communicated messages.

4. The Proposed Algorithm

The main underlying idea of the proposed algorithm is to produce random numbers and exchanging them between sink and sensor nodes so as to detect the Sybil nodes. Generally, the proposed algorithm contains two simple phases that are explained below.

4.1 Configuration

This phase runs before distribution of nodes in the operating environment of the network. According to mechanism given in [19], a single identity is assigned to each sensor node, in the first place. Then, a table, as the one indicated in figure 2a, is loaded on each sensor node and another table, as the one indicates in figure 2b, is loaded on each sink node; the tables are called history. For every sink nodes and sensor nodes, an identity is registered in SinkID and NodeID column of the tables. The number column belongs to random numbers; the initial value of this field for all sensor and sink nodes is null. In the next place, all nodes have to be distributed in the network environment, randomly.

(b)

NodeID	*number*
N1	
N2	
. . .	
Nn	

(a)

SinkID	*number*
SK1	
SK2	
...	
SKm	

Figure 2 – The structure of history tables in sensor nodes (a) and sink nodes (b) memory

4.2 Test

After being distributed in the environment, th**e** sensor nodes began sending "Hello" (to identify the neighbors), routing, data, and … messages. After a period (t), the nodes start moving in the environment and when they arrive at a new point, they start sending the messages (i.e. 'Hello, routing, data messages), again. Thus, each node can detect its existing neighbors, during different periods of network lifetime, by considering these types of broadcasted messages. Testing phase of the proposed algorithm also runs during alternative periods (t) of network lifetime. The testing phase runs as follows: whenever there is a sensor node (N_i) in the vicinity of a sink node (SK_j), the sink node generates a random number (p) and stores it in the number column of its history table if it learns that there is an empty field in the number column of N_i. Then, it sends the random number (p) to N_i, along with a message containing $<< SK_j, p >>$. N_i updates its history as it receives the message; in other words, it registers p in the number field of SK_j. But, if the number field of N_i in SK_j history has already been filled with a random number, like p', (i.e. the sink node (SK_j) has sent a random number (p') to N_i before) the sink node (SK_j) requests the random number from N_i. Accordingly, N_i sends the random number that exists in its history, like p", to the sink node. If p" be equal to p', the sink node considers N_i as a legitimate node; otherwise, it regards N_i as a malicious Sybil node.

Now, consider a scenario in which, SK_j sends p' to a sensor node (N_i) during t_1. Also, assume that an enemy steals legitimate identities (***$N_{i\sim k}$***) from the network and a malicious node is programmed itself to distribute the stolen Sybil identities, i.e. ***$N_{i\sim k}$,*** after being scattered in the network environment. If during $t_l>t_1$ periods, there is a Sybil node (N_i) in the vicinity of a sink node (SK_j), it request the Sybil node (N_i) to return the random number because there is no empty member field for N_i in history of the sink node (SK_j) (it is filled with p'). But if the Sybil node (N_i) generates a random number, since it has no random number available in history for the sink node, it can register the number in its history and return it to the sink node. Hope that the random number be the same number that the sink node (SK_j) has requested (i.e. p'). If so, the Sybil node (N_i) cannot be detected. If not, the sink node marks N_i as a malicious node. In this case, Sybil node's success depends on complexity of the random number. To avoid suspicion to these random numbers by the malicious nodes, a 32- or 64-bit number field can be used.

In another scenario, assume that a sink node (SK_j) sends a random number (p') to a Sybil node (N_i) during t_1 period (i.e. the first time that the sink node (SK_j) identifies a N_i node in its vicinity). Now, if during $t_l>t_1$ periods, the sink node (SK_j) identifies a N_i node in its vicinity, it request the Sybil node (N_i) to return the random number because it has no empty member field for N_i in its history. Since, the N_i node, that is now (during t_l) in the vicinity of SK_j, is a legitimate node (not a Sybil node (N_i)) and has no random number in its history for the sink node (SK_j), it sends a warning message to the sink node. Upon receiving the alarm, the sink node understands that N_i is captured by enemy. Therefore, it considers N_i as a Sybil node. It should be noted that each sink node generates and sends the random number to N_i just and only once; however, it may request the N_i (when the node is in its vicinity) to return the random number several times during the network lifetime.

5. Performance Evaluation and Simulation Results

In this section, we first evaluate the proposed algorithm memory, communication, and processing overheads, then present the simulation results.

5.1 Performance Evaluation

Memory Overheads: in the proposed algorithm, each sensor node requires a memory space with O (m) function and each sink node requires a memory space with O (n) function to store data in history. Since sink nodes are not resource-limited, memory overheads with O (n) function can be imposed on these nodes. Yet, given that the number of sink nodes in most of the sensor networks are generally are too small (less than 10), sensor nodes of the memory overheads tolerate very little memory.

Communication overheads: Assuming that each node has d neighbors, on average, each sink node "sends" or "requests" d random numbers during each time period. Also, each sensor node, sends at least 0 and at most m message for the sink nodes in each time period, during the test phase. Because it may have no sink node or many sink nodes in its vicinity. Therefore, connection overheads of sensor nodes and sink nodes are of O (m) and O (d) type, respectively.

Processing Overheads: in each time period, during the test phase, each sink node has to update its history (which is of O (d x n) time order) per all its existing neighbors and each sensor node requires at most O (m^2) processing time to update its history (by assuming a linear search), as well. Because in any of the time periods during the test phase there may appear m sink nodes in the vicinity.

5.2 Simulation Results

After running the proposed algorithm, its performance is evaluated through a series of tests. The main criterion in the evaluation is detection rate; i.e. the amount of Sybil nodes detected by a security algorithm. What is more, the proposed algorithm performance is compared with those given in [8-10,13,14,16], in terms of average detection rate and average rate of error.

In simulation, it is assumed that the network includes n sensor nodes and m sink nodes which are randomly distributed in 100 x 100 m^2 area. The function area has W=5 malicious hostile nodes (Sybil attack runners) and each malicious node creates S Sybil identity. So, (W x S) Sybil nodes are available in the network. All the nodes (normal and malicious) has equal radio range (r=10). In addition, the mobility model of [21] is employed for the nodes movement in the function area. In order to be sure of the results validity, each test is repeated 100 times and the final result is the average of these 100 tests.

Experiment 1: parameters considered in this experiment are n=30, S=20, and m=1, 2, 3. Detection rate of the proposed algorithm is evaluated in time periods 25 to 200 during the test phase. Figure 3 indicates the experiment results. The results indicate that increasing time periods of the test phase increases the Sybil nodes detection rate. For example, when the number of sink node equals to m=1, detection rates of time period 25, 100, and 200 are about 27%, 88%, and 100%, respectively. The reason is clear; assume that enemy has captured N_i and its malicious node creates a Sybil node with N_i identity, after being distributed in the network. In this case, a sink node can detect Sybil N_i only if it faces with both legitimate N_i and malicious hostile node (in its vicinity) during the test phase (not necessarily in a certain time period). Accordingly, by increasing the number of phase test periods, it is more probable that the sink node faces with both N_i and the malicious node.

Also, since, in the proposed algorithm, sink nodes detects Sybil nodes in a fully independent way, its detection rate increases by increasing the number sink nodes (m). Figure 3 clearly indicates the test results.

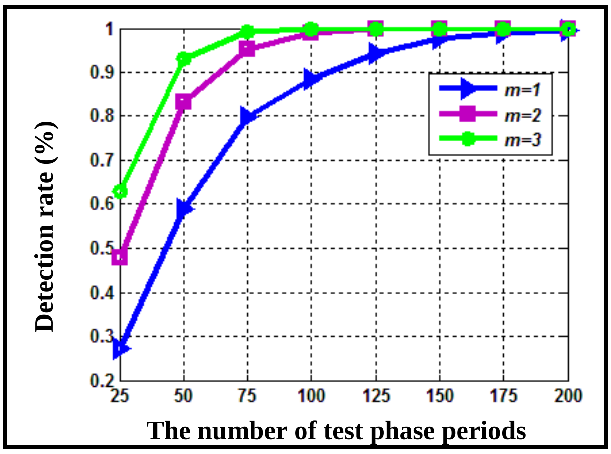


Figure 3 – Detection rate of the proposed algorithm per different parameter (m) values and different test phase periods

Experiment 2: This experiment is to evaluate the effect of Sybil identities number, distributed by malicious nodes (S), on the proposed algorithm performance. Parameters considered in this experiment are n=300 and m=1. Detection rate of the proposed algorithm is evaluated for Ss 4 to 20 (by increasing 4 units per step). Figure 4 indicates the experiment results for time periods 25 to 200 during the test phase. The experiment results prove that changes of S have no significant effect on detection rate of the proposed algorithm because what matters the most in this algorithm is the presence of malicious and legitimate nodes, the identities of which is captured by the enemy, in the vicinity of sink nodes during the test phase. But, considering the Sybil attack model assumed here (i.e. “simultaneous” model), whenever the malicious node moves to a new location in the network, it sends “Hello”, routing, etc. messages, per each of its Sybil identities. So, the number of distributed Sybil identities of the malicious node does not matter; however, it is enough to be in the neighboring environment of the both malicious and legitimate nodes, with captures identity, only once, then the sink node can detect the Sybil nodes.

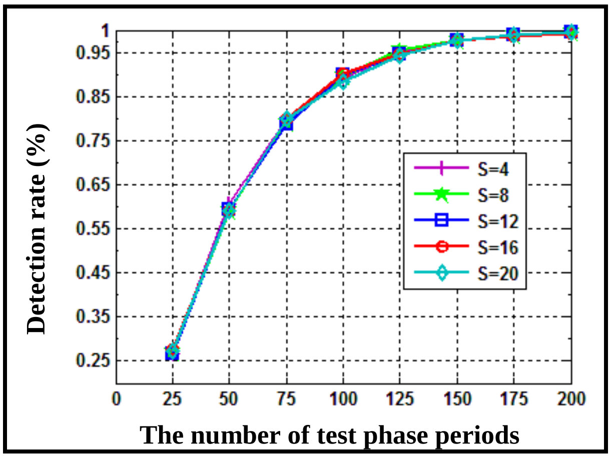


Figure 4 – the effect of parameter (S) on detection rate of the proposed algorithm

Experiment 3: This experiment is to evaluate the effect of network nodes number (n) on the proposed algorithm performance. Parameters considered in this experiment are S=10 and m=1. Detection rate of the proposed algorithm is evaluated for ns 100 to 500. Figure 5 indicates the experiment results for time periods 25 to 200 during the test phase. The experiment results prove that network nodes number (n) has no significant effect on detection rate of the proposed algorithm because, unlike other algorithms, such the one developed in [9], the proposed algorithm is not based on network density but on confrontation of malicious and legitimate nodes, the identities of which is captured by the enemy, in the vicinity of sink nodes. Therefore, increase or decrease of the number of nodes in the network leaves no effect on detection rate of the proposed algorithm.

Experiment 4: in this experiment**,** the proposed algorithm performance is compared with others in terms of **average detection rate and average rate of error.** Figure 6 and figure 7 indicate the average detection rate and average rate of error. The average detection rate of the proposed algorithm, [8], and [16] are almost 100% which is better than others. Also, it is worth noting that, unlike other algorithms, the proposed algorithm makes no error in detecting Sybil nodes. Whereas, error rates of other algorithms in [8] and [16] are 6% and 5%, respectively. It is because the other algorithms are based on information collected from the neighborhood or on RSSI. So, they may have error in detecting Sybil nodes. But, the underlying idea of the proposed algorithm is confrontation of malicious nodes with sink and legitimate nodes, the identities of which is captured by the enemy.

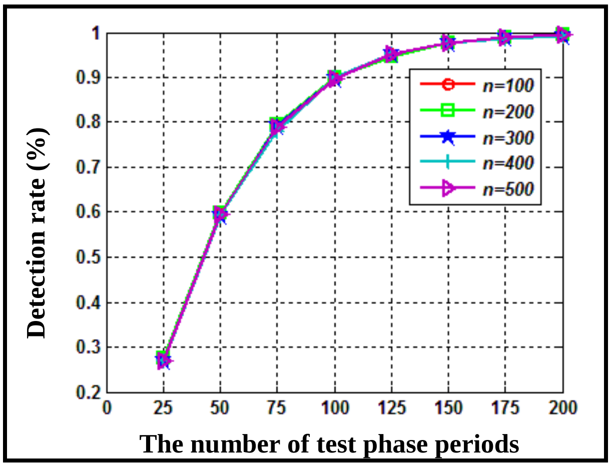


Figure 5 – The effect of parameter (S) on wrong detection of the proposed algorithm

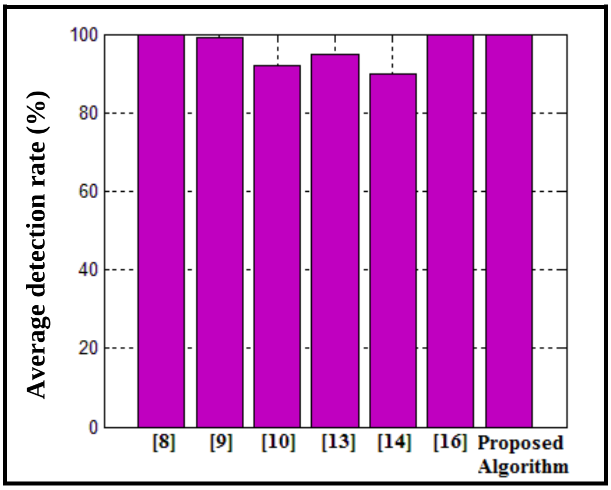


Figure 6 – Comparison of the average detection rate of the proposed algorithm with other algorithms

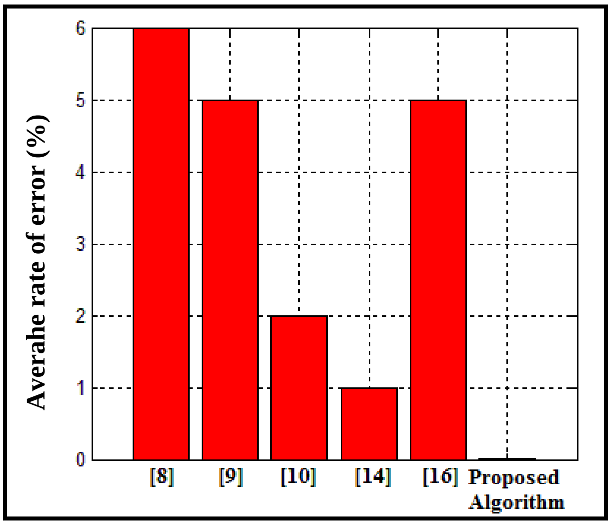


Figure 7 - Comparison of the average error rate of the proposed algorithm with other algorithms

6. Conclusion

The current research proposes a new lightweight algorithm for detecting Sybil attack in Mobile Wireless Sensor Networks using sink nodes. The main underlying idea of the proposed algorithm is generate random numbers by sink nodes and exchange them between sink and sensor nodes to detect Sybil nodes. The proposed algorithm is implemented to be assessed in terms of detection and error rates efficiency in a series of experiments. Comparison of the experiment results with the results of other available algorithms revealed optimal performance of the proposed algorithm.

7. REFERENCES

[1] Akyildiz Ian F. and Kasimoglu Ismail H., "Wireless sensor and actor networks: research challenges", in: Proceedings of the Ad Hoc Networks 2, pp. 351–367, 2004.

[2] Karlof C. And Wagner D, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, in: Proceedings of the AdHoc Networks, pp. 299-302, year 2003.

[3] Padmavathi G. and shanmugapriya D, "A survey of attacks, security mechanisms and Challenges in Wireless sensor networks", in: Proceedings of the International Journal of Computer Science And Information Security (IJCSIS), Vol. 4, No. 1 & 2, August 2009.

[4] Douceur J. R., “The Sybil attack”, in: Proceedings of the Douceur J. R., “The Sybil attack”, in: Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS '02), 2002.

[5] Newsome J., Shi E., Song D. and Perrig A., “The Sybil attack in sensor networks: analysis and defenses”, in: Proceedings of the International Symposium on Information Processing in Sensor Networks, pp. 259–268, April 2004.

[6] D. Liu, P. Ning, “Establishing pairwise keys in distributed sensor networks”, in: Proceedings of the ACM Conference on Computer and Communications Security, pp. 52–61, October 2003.

[7] Zhong S., Li L., Liu Y. G. and Yang Y. R., "Privacy-preserving location based services for mobile users in Wireless Networks", In: Proceedings of the Technical Report YALEU/DCS/TR-1297, Yale Computer Science, 2004.

[8] Demirbas M. and Song Y., "An RSSI-based scheme for Sybil attack detection in wireless sensor networks", In: Proceedings of the IEEE Computer Society International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 570–574, 2006

[9] Ssu K. F, Wang W. T. and Chang W. C., “Detecting Sybil attacks in wireless Sensor Networks using neighboring information”, in: Proceedings of the Computer Networks 53, pp. 3042–3056, 2009.

[10] Chen S., Yang G. and Chen S., “A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks”, in: Proceedings of the International Conference on Communications and Mobile Computing, 2010.

[11] Misra S. and Myneni S., “On Identifying Power Control Performing Sybil Nodes in Wireless Sensor Networks Using RSSI”, in: Proceedings of the IEEE Communications Society, 2010. http://www.csee.usf.edu/~labrador/Share/Globecom/DATA/03-384-04.PDF

[12] ZHANG Y., FAN K.-.F., ZHANG S.-B. and MO W., ”AOA based trust evaluation sheme for Sybil attack detection in WSN”, in: Proceedings of the journal on Application Research of Computers, 2010.

[13] Muraleedharan R., Ye X. and Osadciw L.A., “Prediction of Sybil Attack on WSN Using Bayesian Network and Swarm Intelligence”, in: Proceedings of the Wireless Sensing and Processing, Orlando, FL, USA, March 2008.

[14] Jangra A., Swati, Priyanka, “Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS)”, in: Proceedings of the International Conferences on Advances in ICT for Emerging Regions(ICTer2011), 2011.

[15] Jiangtao W., Geng Y., Yuan S. and Shengeshou C., “Defending Against Sybil Attacks Based on Received Signal Strength in Wireless Sensor Networks”, in: Proceedings of the journal of elctronics, Vol. 17,No. 4, Oct. 2008.

[16] Jamshidi, M., Esnaashari, M. and Meybodi, M. R., "An Algorithm for Defending Sybil Attacks based on Client Puzzles and Learning Automata for Wireless Sensor Networks", in: Proceeding of 18th National Conference of Computer Society of Iran , Sharif University, Tehran, Iran, March 14-16, 2013.

[17] Jamshidi, M., Esnaashari, Nasri A., Hanani A. and Meybodi, M. R., "Detecting Sybil Nodes in Mobile Wireless Sensor Networks using Observer Nodes”, in: Proceeding of 10th International ISC Conference On Information Security &Cryptologhy, Computer Society of Iran , yazd University, yazd, Iran, August 29-30, 2013.

[18] Rezai A., Jamshidi M. and AkbariTorkestani J., "A lightweight and robust algorithms to detect Mobile Sybil Nodes in Moblie Wireless Sensor Networks using Information about the mobility of nodes”, in: Proceeding of 10th International ISC Conference On Information Security &Cryptologhy, Computer Society of Iran , yazd University, yazd, Iran, August 29-30, 2013.

[19] Butler K. and et al., “Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems”, in: Proceedings of the IEEE transaction on parallel and distributed systems, Vol. 20, 2009.

[20] Piro C., Shields C. and Levine B. N. , ”Detecting the Sybil Attack in Mobile Ad hoc Networks”, in: Proceedings of the Securecomm and Workshops, pp 1-11, 2006.

[21] Yu C. M., Lu C. S. , and Kuo S. Y., “Mobile Sensor Network Resilient Against Node Replication Attacks” In: Proceedings of the IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 2008.

International Journal of Computer Applications Technology and Research
Volume 5– Issue 7, 439 - 442, 2016, ISSN:- 2319–8656

E-government Security Models

Omar A. Ali
Department of Information Systems
Najran University
Najran KSA

Talaat M. Wahbi
Department of Computer Science and Technology
Sudan University of Science and Technology
Khartoum, Sudan

Izzeldin M. Osman
Department of Computer Science
Sudan University of Science and Technology
Khartoum, Sudan

Abstract: E-government security is a key problem to restrict the construction and development of E-government systems in any country over the world. E-Government security models are widely used in the implementation and development of e- government systems. Due to the deference situation of the countries over the world there are various security models applied in each country. This paper reviews different security models in e-government in order to determine important parameters for e-government strategic planning.

Keywords: E-government, security model, ICT, layers, sub-layer

1. INTRODUCTION

Dependency on Information and Communication Technology (ICT) for supporting core operations to both government and private sector is increasing [1]. Similarly, organization's critical information has developed into a key strategic asset in a competitive world [2]. Nevertheless, the pace of ICT advancement such as development, deployment and use of e-government infrastructures is much faster than the development and deployment of security services, including technical and the existing and new emerging security risks [3, 4]. Technical security aspects include hardware and software solutions such as Access control and Antivirus mechanisms [5, 6, 7]. The application of information security principles in an e-government environment is a complex, multidimensional issue involving people, technology and processes. E-government security is considered one of the crucial factors for achieving an advanced stage of e-government. As the number of e-government services introduced to the user increases, a higher level of e-government security is required.

2. REVIEW

In order to get the maximum decrease of data breaches and get the maximum protection of critical data when using e-government systems in any country over the world there should be a security model to satisfy this purpose. The security models of E-government may be based on layers [9], cloud computing [10], based on service-oriented architecture [15], access control policy [11], and security system based on information security model [12].

2.1 The Five Security Layered-Model in Dubai

In this model there are five layers. Each layer will mitigate group of threats related to an e-services. The model is composed of technology layer, policy layer, competency layer, operational and management layer, and decision layer. The technology layer for example will address all the technological threats while the policy and competency layers will address the threats on an e- service related to the human aspect. Each layer is composed of detailed layer which is called the sub-layer of the main layer [8]. See figure 1 showing the E-government security model in Dubai.

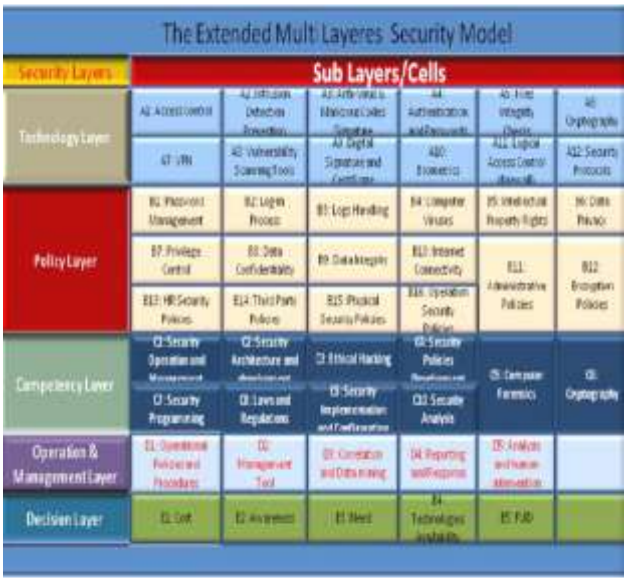

The Extended Mult Layeres Security Model
Security Layers
Sub Layers/Cells
Technology Layer
A1: Access control
A2: Intrusion Detection Prevention
A3: Anti-Virus & Malicious Codes Signature
A4: Authentication and Passwords
A5: Files Integrity Checks
A6: Cryptography
A7: VPN
A8: Vulnerability Scanning Tools
A9: Digital Signature and Certificate
A10: Biometrics
A11: Logical Access Control (Firewall)
A12: Security Protocols
Policy Layer
B1: Password Management
B2: Logon Process
B3: Logs Handling
B4: Computer Viruses
B5: Intellectual Property Rights
B6: Data Privacy
B7: Privilege Control
B8: Data Confidentiality
B9: Data Integrity
B10: Internet Connectivity
B11: Administrative Policies
B12: Encryption Policies
B13: HR Security Policies
B14: Third Party Policies
B15: Physical Security Policies
B16: Operation Security Policies
Competency Layer
C1: Security Operation and Management
C2: Security Architecture and development
C3: Ethical Hacking
C4: Security Policies Development
C5: Computer Forensics
C6: Cryptography
C7: Security Programming
C8: Laws and Regulations
C9: Security Implementation and Configuration
C10: Security Analysis
Operation & Management Layer
D1: Operational Policies and Procedures
D2: Management Tool
D3: Correlation and Data mining
D4: Reporting and Response
D5: Analysis and human intervention
Decision Layer
E1: Cost
E2: Awareness
E3: Need
E4: Technologies Availability
E5: R&D

Figure. 1 E-government security model in Dubai

2.2 Government Cloud Computing Proposed Model: Egyptian E-Government Cloud Computing

The proposed hybrid model for Egyptian E-Government Cloud Computing consists of three computing clouds; Inter-Cloud computing, Intra- Cloud computing and Extra-Cloud computing, Figure 2. The three cloud models are analogs to the terms Internet, Intranet and extranet in their functionality, operation and management. Intra-Cloud computing "I**A**CC" is a private cloud which is dedicated to a single national entity cluster, (see Figure 3). Members of that cluster are the only legitimate users. Extra-Cloud computing "E**X**CC" is a community cloud that enables entities from different clusters to integrate and to aggregate their work as required. There are two types of E**X**CC. The first type connects multiple I**A**CC of a specific national entity cluster, Figure 3. The second type connects different national entity clusters that differ in their functions and services, (see Figure 2). Inter-Cloud computing "I**E**CC" is a public cloud that enables any user (citizen, guest, organizations) to require specific requests and receives their responses or outcomes, (see Figure 2). In I**E**CC, it is expected to store the least sensitive data and to run the related application software.

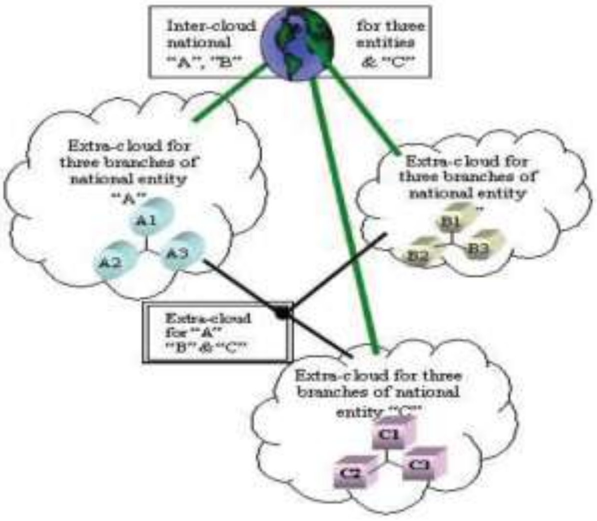

Inter-cloud national "A", "B"
for three entities & "C"
Extra-cloud for three branches of national entity "A"
A1
A2
A3
Extra-cloud for three branches of national entity
B1
B2
B3
Extra-cloud for "A" "B" & "C"
Extra-cloud for three branches of national entity "C"
C1
C2
C3

Figure. 2 Proposed model for Egyptian E-Government Cloud Computing

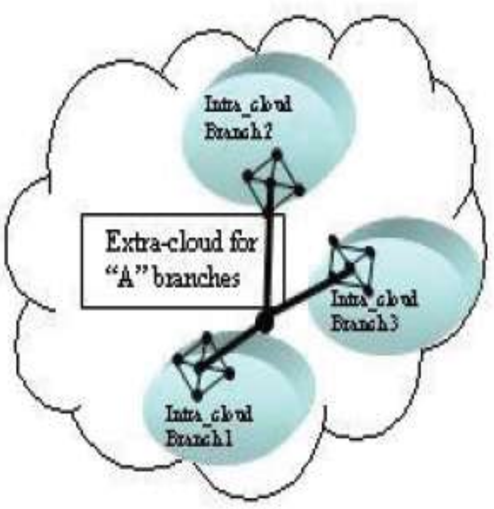


Figure. 3 IACC and EXCC for National entity A.

2.3 A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania

The proposed secured e- Government maturity model consists of four layers, namely: (1) secured digital presence, (2) secured interaction, (3) secured transaction, and (4) secured transformation. The implementation of the proposed model is neither based on a specific technology/protocol nor a certain security system/product, but rather an approach towards a structured and efficient implementation of those technologies. The security layers include technical and non-technical security control elements. The proposed security layers are further described in the following paragraphs. [10]

2.3.1 Secured Digital Presence

This stage involves simple provision of government information through website (static) with basic information that the citizen can access [11]. This is a one-way communication between governments, businesses and citizens. Generally, the information provided by organizations at this stage are public and normally with zero security. At this stage, the security layer should have the ability to verify e- Government services identity in order to build trust between government agencies and users. The users would like to be sure that they are connected to the e-Government service belonging to the administration in question [12].

2.3.2 Secured Interaction

At this stage the interaction between government and the public (Government-to-Citizens and Government-to-Businesses) is stimulated by various applications. Citizens can ask questions via e-mail, use search engines and download forms and documents [12]. The communication is performed in two ways, but the interactions are relatively simple and generally revolve around information provision. At this stage, the security layer should have the ability to authenticate a user/ citizen asking for a service. The most important security aspects at this stage are identity authentication, availability and integrity.

2.3.3 Secured Transaction

At this stage public organizations provide electronic initiatives and services with capabilities and features that facilitate clients to complete their transactions in full without the necessity of visiting government offices [37]. The public can carry out their financial transactions with the government Such services also allow the government to function in a 24/7 mode. The most important security aspects at this stage are personal information confidentiality, identity authentication, availability, non-repudiation, accountability and integrity.

2.3.4 Secured Transformation

This stage allows users of e-Government services to interact with government as one entity instead of Information systems are integrated, and the citizens' individual government organizations [14]. can get services at one virtual counter. The integration of information systems can result in situations where the privacy of individual citizens is in danger. The most important security aspects of this stage are personal information confidentiality, identity authentication, availability, nonrepudiation, accountability and integrity. At this stage, the security layer should restrict the utilization of personal information, and secure such information from access by unintended parties. A government agency should be able to authenticate another government agency that requires a service on behalf of the users.

2.4 A Security E-government Model Based on Service-oriented Architecture

Service-oriented architecture is an IT architectural style that supports integrating business as linked services which users can combine and reuse them in the production of business applications [15]. It provides an effective way for constructing loose coupled web services. It relies on services exposing their functionality via interfaces that other services can understand how to utilize those services. SOA logical architecture is shown in Figure 4 [16].

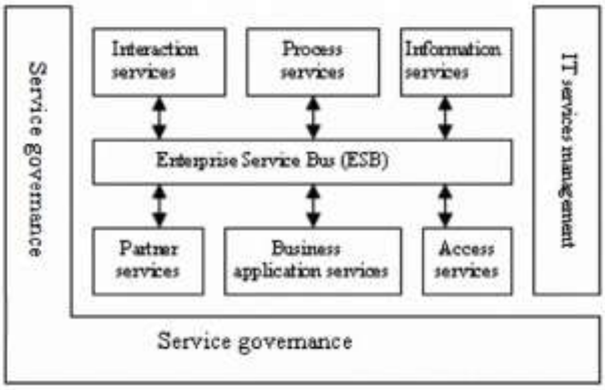


Figure. 4 SOA logical architecture

The SOA technology framework to integrate E-government: using BEPL implement work process; realizing seamless integration between services by ESB. Taking the case of online application processing, a scheme of integration E-government system based on SOA is shown as Figure 5. [16]

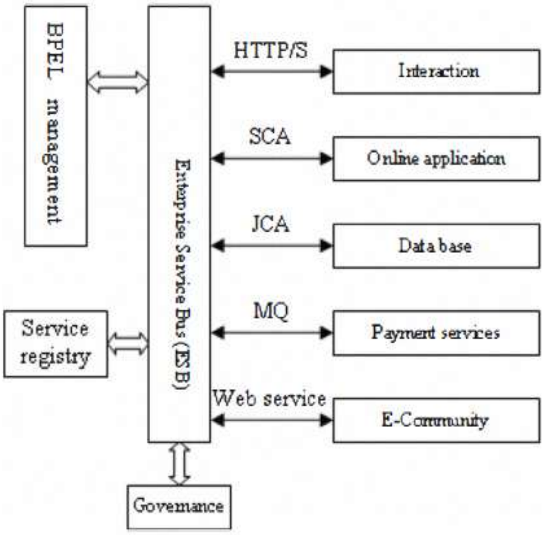


Figure. 5 A scheme of integration E-government system based on SOA

2.5 Research on Role-Based Access Control Policy (RBAC) of E-government

The access control system includes subjects, objects and access control policy, and their relationship is shown in figure 6 [17].

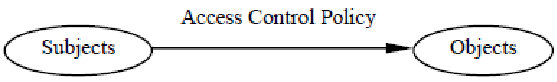


Figure. 6 Access Control System Model

The RBAC is a new access control technique and notion. It is the development and amelioration of DAC and MAC, and it has been regarded as an effective measure to resolve resource unified access control of large information systems by the public. The RBAC contains five kinds of entities, such as users, roles, constraints, permissions, and sessions. In the RBAC model, it injects the idea of roles between users and access permissions, and a user connects with one or more specific roles, and a role connects with one or more permissions, and roles can be created or canceled according to actual working requirements. The sessions show the relationship between users and roles. The users should activate roles by creating sessions every time and get the specific resource access authorities as shown in Figure 7 [18-19].

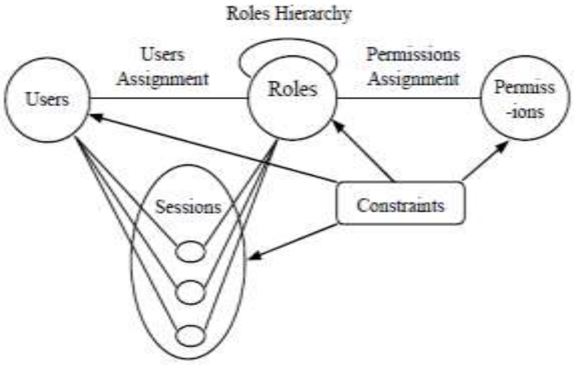


Figure. 7 Basic RBAC Model

2.6 Security System based on Information Security Model

The system is designed through modularization and it is mainly divided into initialization module, management module and various application modules. In which, the initialization module is used to manage the original data of the initial management module and various application modules, the management module is used to manage the content which has effect in the overall system, such as the users, privileges and a series of rules in the system. Various application modules work together by using the initialized data and through the transmission media to complete the overall function of the system. The secure e-government system structure is shown in Figure 8.

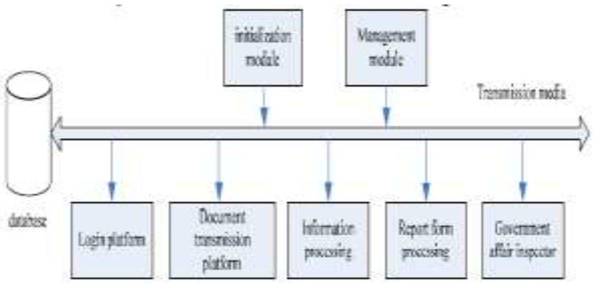


Figure. 8 Secure e-government system

3. CONCLUSION

Based on the research that led up to this paper, the security model for e-government that adopt layers in its structure is more coherent and comprehensive because of covering all threats that faced e-government in each country. Also this type of models is so easy to be understandable to the employees in any organization.

4. REFERENCES

[1] G. Dhillon, (2000). *Challenges in managing Information Security in the millennium,* Idea Group Publisher, Las Vegas, USA.

[2] S. Woodhouse, (2007). Information Security: End User Behavior and Corporate Culture, 7th *International Conference on Computer and Information Technology*. (IEEE). Pp 767-774. University of Aizu. Fukushima, Japan.

[3] G. Karokola, L. Yngström, & S. Kowalski, (2010). A Comparative Analysis of e-Government Maturity Models for Developing Regions: The Need for Security Services. *International Journal of Electronic Government Research*. **8**: 1-25.

[4] P. W. Anderson. (2001). Information security governance. *information security technical report*. **6**: 60 – 70.

[5] G. McGraw, (2005). *Software Security*. *Volume1*. Addison-Wesley software. USA.

[6] M. Bishop, (2006). *Computer Security – Arts and Science*. Volume1. Addison-Wesley, USA.

[7] M. Wimmer, & B. Bredow, (2001). E-Government: Aspect of Security on different layers, In: *Proceedings. 12th International Workshop.* (Database and Expert Systems Applications) Pp 350-355. IEEE, Linz University., Austria

[8] Al-Azazi, S (2008). *Amulti-layer model for e-government information security assessment*. Grandfield university, dubai

[9] Hana, M (2013). E-Government Cloud Computing Proposed Model: Egyptian E_Government Cloud Computing. *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. Pp 848-852. Electrical and Communication Department Canadian International College ElSheikh Zaid. Egypt

[10] Waziri, M. Yonah , Z. (2014). *A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania*. *Advances in Computer Science: An International Journal* **3**: 98-106.

[11] G. Karokola and L. Yngström, (2009). Discussing E-Government Maturity Models for the Developing World-Security View. *Information Systems Security Association* Pp81-98.

[12] Zhang, F. (2008). Design of E-government Security System based on Information Security Model. *2008 International Conference on Advanced Computer Theory and Engineering*. **(***Research Center of Cluster and Enterprise Development***)** **Pp**359-362. Jiangxi University of Finance and Economics. China

[13] www.clknet.or.tz J. Yonazi, Adoption of Transactional Level e-Government Initiatives in Tanzania. (Retrieved 13Apr2014)

[14] www.utumishi.go.tz, President's Office, Public Service Managements, Tanzania e-Government Strategy, ed, 2012. (Retrieved 10Feb2013)

[15] Erl, T, (2005). *Service-oriented Architecture: Concepts, Technology, and Design.* Volume2. Upper Saddle River: Prentice Hall PTR, USA

[16] Ziyao W, Junjie N, Z Duan, (2008). SOA core technologies and application, Publishing House of Electronics Industry, Beijing, Pp.495-497,

[17] L Lin, Yongzhao Z, Yi N. (2006) Improved RBAC model based on organization. Journal of Jiangsu University (Natural Science Edition) **27**(2):147-150

[18] Zeng Zhongping, Li Zonghua, Lu Xinhai. (2007). The Access Control Policy Study of E-government Information Resource Based on RBAC. *Journal of Information*, **10**:39-41

[19] Barka E, Sandhu R S. (2000). Framework for role-based delegation models. *In: Proc. of the 16th Annual Computer Security Application Conf. IEEE Computer Society Press*. Pp 168-176

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 443 – 447, 2016, ISSN: - 2319-8656

Design and Implementation Security Model for Sudanese E-government

Omar A. Ali
Department of Information Systems
Najran University
Najran KSA

Talaat M. Wahbi
Department of Computer Science and Technology
Sudan University of Science and Technology
Khartoum, Sudan

Izzeldin M. Osman
Department of Computer Science
Sudan University of Science and Technology
Khartoum, Sudan

Abstract: Security is one of the most important issues in E-government projects. E-government applications will be increasingly used by the citizens of many countries to access a set of services. Currently, the use of the E-government applications arises many challenges; one of these challenges is the security issues. E-government applications security is a very important characteristic that should be taken into account. This paper makes an analysis over the security as required for E-government and specify the risks and challenges that faces E-government projects in Sudan. Finally, the study has proposed security model for Sudanese E-government. The proposed security model for the Sudanese electronic government is a four layers' model that is divided into sub layers. Each layer will mitigate group of threats related to an e-services. The model is not generic; it cannot be applied by other countries. It is precisely designed for Sudanese situation.

Keywords: E-government, security model, countermeasures, NIC, IT infrastructure, managerial layer

1. INTRODUCTION

E-government security is facing a wide range of threats. The threats may be technical or non-technical. Modeling is the specific description of the link between the objective world and the abstract things. Constructing the security model of E-government for any country depends on its situation. Holistic security is a form of security which operates on multiple, fully integrated levels or layers. This approach to security can be taken to secure a structure, a computer network, a campus, and any number of other things which might need securing. The underlying idea behind holistic security is that systems need to be considered as wholes to achieve the greatest level of security; while it is important to be aware of individual aspects of a system, the ways in which these aspects work together are also a key part of a security system. There are four layers in Sudanese electronic government security proposed model, and each layer is composed of sub-layers. The purpose of this paper is to construct a comprehensive model which will consist of multiple layers that complement each other.

2. STATEMENT OF THE PROBLEM

The Electronic Government is the high efficient, good quality management and service, in which the government employs technology of modern network communication and computer to realize its functions on network by such means of reduction, optimization, conformity and recombination. Because E-government is involved in government policy and the country's secrets, people always pay close attention to its security. How to ensure E-government's security is a longstanding key problem for E-government. The security model for E-government of Sudan can help to guide IT managers recognise the technological and organisational requirements for securing E-government in public sector organisations. The security model for Sudanese E-government can also help the decision makers to set a vision and strategic action plan for future direction in the information technology age through identifying key elements and stages for action.

3. RELATED WORK

Many studies have been conducted to propose security models of E-government in deferent countries over the world. Al-Azazi, in a study presents five security layers models in Dubai E-governments [3]. The model is composed of technology layer, policy layer, competency layer, operational and management layer, and decision layer. Each layer is composed of detailed layer which is called the sub-layer of the main layer. Hana, in her study proposed hybrid model for Egyptian E-Government Cloud Computing consists of three computing clouds; Inter-Cloud computing, Intra- Cloud computing and Extra-Cloud computing [4]. Waziri, and Yonah, in their study proposed secured E- Government maturity model consists of four layers, namely: (1) secured digital presence, (2) secured interaction, (3) secured transaction, and (4) secured transformation [5]. Ziyao Junjie, Duan introduced service-oriented architecture which is an IT architectural style that supports integrating business as linked services which users can combine and reuse in the production of business applications [6]. Lin, Yongzhao and Yi introduced the access control system which includes subjects, objects and access control policy, and their relationship [7].

4. MATERIALS AND METHODS

4.1 Study area

Sudan is located in the north-eastern part of Africa (see Figure 1), and occupies the central region between Africa and the Arab World. The location results in Sudan’s unique characteristics, as it is the main passage between north and south of Africa. Sudan was also the main route for the pilgrim and trade convoys that crossed from the west of Africa to the

Holy Lands in Makah, until the middle of the current century [1].

4.2 The data

A preliminary study is an initial study to gather basic information –not full information- to specify the research problem. The main aim of a preliminary study for this research is to make a general idea about the security of e-government in Sudan. Also an interview with specialists in National Information Centre (NIC) which is a responsible body for E-government project in Sudan will be conducted, there are many detailed points related to this issue. Direct observation also is an important resource to gain information about the E-government security in Sudan.

Figure. 1 Map of Sudan

5. THE PROPOSED MODEL

Implemented the research methodology consists of series of actions or steps necessary to effectively carry out research and the desired sequencing of these steps. The chart shown in (Figure 2) will illustrate the implemented research methodology. The following section describes each step.

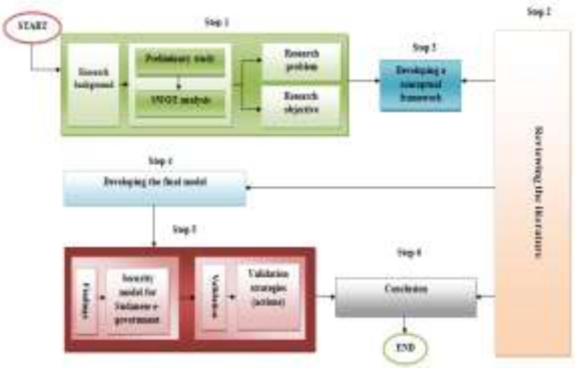


Figure. 2 Shows the implemented research methodology

Step 1: Conducting the preliminary study, SWOT analysis and identifying the research problem to achieve the research objectives

After establishing the research background, a pilot study was conducted with state e-government authorities, IT professionals; and academics. The findings from the preliminary study directly contributed to building the initial conceptual framework. Additional data was gathered through informal dialogue, government agency websites, publications and articles highlighted issues and challenges related to a variety of aspects; IT infrastructure, managerial, legal and technical. The interview was then collated data and analyzed using the SWOT tool of analysis.

Step 2: Reviewing the literature

The literature review explaining the existing security models addressing policies and the security triad (confidentiality, integrity, availability) which act as the high level objectives of any security architecture or model. Different types of models were analyzed. Models addressing confidentiality or integrity only were such as BLP or Biba were analyzed. Social and human behavioral model and theories were searched to build the concept of the human aspect in the information security field. In addition, e-government assessment and stages of growth, models and frameworks developed in e- government and other disciplines (IT and IS) were thoroughly reviewed.

The review of the literature led to different ideas on how to pursue constructing the new model. More significantly, was the deep review of the key issues that have impact upon the adoption of new technology in general, and e-government innovation in particular; such as, organizational and environmental issues. The majority of the literature was addressing technological security solutions or approaches to solve issues related to data integrity or confidentiality. These technological solutions were presented as architectures required or programmes to be installed in the IT infrastructure.

Step 3: Developing a conceptual framework

After identifying the research problem and reviewing the related literature the initial framework was provided. The framework is based on the IT infrastructure, managerial, legal and technical. The framework and its critical factors according to the initial findings from the SWOT analysis of the preliminary study, combined with the identified factors and key elements from the literature review were constructed. The development of the conceptual framework step is a major step in theory building and it is considered a type of intermediate theory [2], that attempts to connect all aspects of inquiry (problem definition, purpose, literature review methodology, data collection and analysis). The development of the initial conceptual framework will help develop understanding of the research problem and lead to developing the final model.

Step 4: Developing the final model

In this step of research, the details of each category of challenges and barriers to e-government in Sudan were specified according to its source. The information which was collected from interviewees, observations and documents were formulated into layers, and then these layers were focused studied to provide sub-layers into each category of the layer.

Step 5: Validation

In this step three actions have been implemented in the same time.

Action 1: According to specialists the security layers and sub-layers that mentioned in this research were specified.

Action 2: The criteria that extrapolated from Wood's book [8] for the success of the model were set.

Action 3: The guidelines of modeling presented by [9] were followed.

Step 6: Drawing conclusion

This is the final step of The implemented research methodology. See figure 2.

6. RESULTS

6.1 The security layers, risks and countermeasures

The idea of this model is stemmed from the risk analysis that facing the Sudanese electronic government are listed in the second column of the table 1. The third column of the table 'countermeasures of risks' compose the sub-layer of the model. The collection of the same issues (sub-layers) that mentioned in the third column of the table1 are collected together to form the main layer of the model which are listed in the first column of the table 1 and figure 1.

Table. 1 Illlustrates the layers, risk analysis and Countermeasure of risks

Layer	Risk analysis	Countermeasure of risks
Technical layer	Unauthorized access to a place or other resource.	• Access control • Authentication password
	Information interception	• Cryptography • Training and awareness
	Information tampering	• Authentication password • Using tamper-resistant protocol across communication links • Secure communication links with protocols that provide message integrity. • Cryptography
	Denial of services attacks	• Analysis tools • Monitoring tools • Using resource and bandwidth throttling techniques • Validate and filter input
	System resources stealing	• Access control • Authentication password • Analysis tools • Monitoring tools
	Information faking	• One-time password • Cryptography
IT infrastructure layer	Lack of e-government projects	• Availability of staff skilled • Reliability of infrastructure • Consultation • Software houses
		•
Managerial layer	Lack of e-government projects	• Budget • Policies and mechanism to enforce it • Willingness to change in top management and administration • Conflict of interest
Developing legislative protection and law	Lack of e-government projects	

6.2 The security layers for Sudanese e-government

In order to reach to a comprehensive method to check the security requirements for any electronic enabled organization to allow or not the interchange of information with other e-organizations in Sudan; the multiple security layer was proposed. (See figure 3).

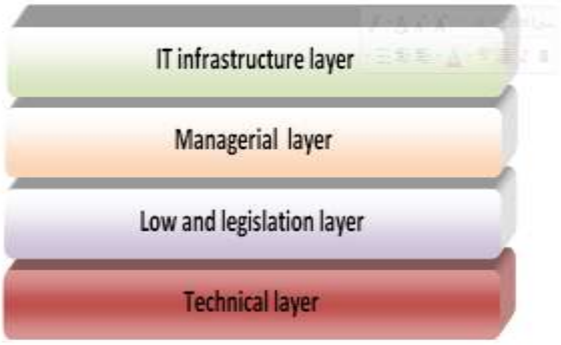


Figure. 3 Illustrates the security layers for Sudanese e-government security model

Any model contains more than one level or layer of security is comprehensive model, and prevent organization from wide range of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services. For example, the technical layer will address all the technological threats while the IT infrastructure will address the threats on e-services related to the requirements that are important to continuity to e-government projects. There are four security layers that contribute in construct the security model for Sudanese security e-government model see figure 3. The model extracted from the interviews and collected data from the responsible body of the e-government projects in Sudan. Each layer of the model contains of detailed layer or sub-layer (see Figure 4).

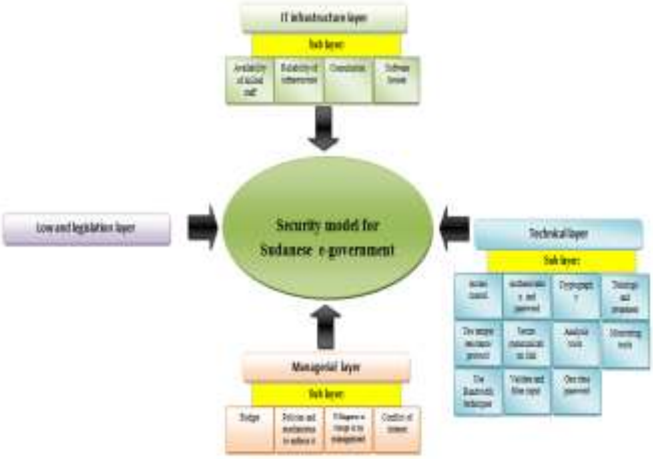


Figure. 4 Illustrate the sub layer of the model

The final model in this research composed of vertical axis that represent the main layers and horizontal axis that represent the sub-layers. The main layers (vertical axis) are positioned according to Sudanese security situation, they are the aspects or risks that facing the security of e-government in Sudan. The sub-layers (horizontal axis) are detailed layers with respect to each main layer. The final model is a coherent and understandable model because of its structure vertical and horizontal axis. (See Figure 5).

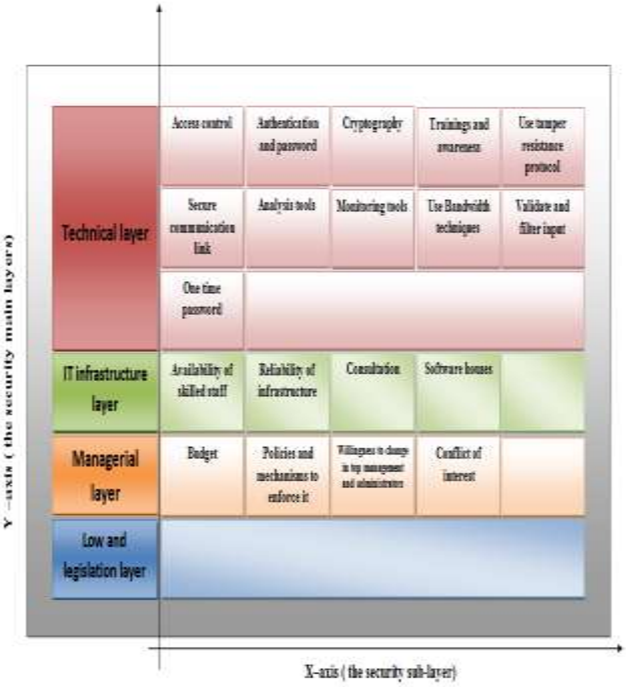

Technical layer
Access control
Authentication and password
Cryptography
Trainings and awareness
Use tamper resistance protocol
Secure communication link
Analysis tools
Monitoring tools
Use Bandwidth techniques
Validate and filter input
One time password
IT infrastructure layer
Availability of skilled staff
Reliability of infrastructure
Consultation
Software houses
Managerial layer
Budget
Policies and mechanisms to enforce it
Willingness to change in top management and administrators
Conflict of interest
Low and legislation layer
Y –axis (the security main layers)
X-axis (the security sub-layer)

Figure. 5 Illustrate the layers and sub-layers of e-government security model for Sudan

7. THE MODEL EVOLUTION

Figure 6 depicts the evolution of the final model from the risks specification stage to the last one.

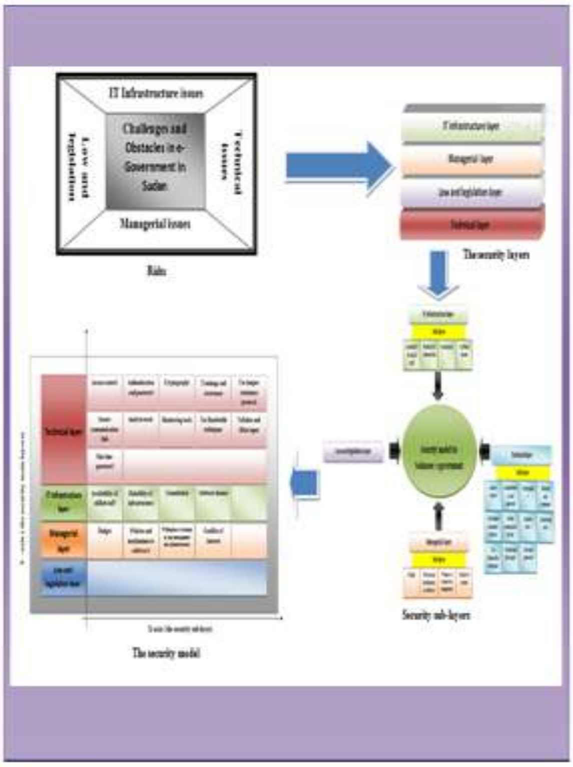


Figure. 6 Illustrates the stages of the model to reach the final model

8. CONCLUSION

The purpose of this paper is to design the security model for Sudanese electronic government. The model with more than one aspects of security is a comprehensive model. All factors that affected the security issue in Sudanese electronic government were found and formed in applicable form in any organization in Sudan.

9. ACKNOWLEDGMENTS

Deep thanks to Prof. Izzeldin M. Osman and Dr Talaat M. Wahbi for their support

10. REFERENCES

[1]http://www.sudan.gov.sd/index.php/en/pages/details/57/About%20Sudan#.ViO_v27evW4 (retrieved 18 Oct 2015)

[2] Carroll, J. M. and Swatman, P. A. (2000). Structured-case: a methodological framework for building theory in information systems research, European Journal of Information Systems, 9: 235-242.

[3] Al-Azazi, S (2008). Amulti-layer model for e-government information security assessment. Grandfield university, dubai.

[4] Hana, M (2013). E-Government Cloud Computing Proposed Model: Egyptian Government Cloud Computing. International Conference on Advances in Computing. Communications and Informatics (ICACCI). Pp 848-852.

Electrical and Communication Department Canadian International College ElSheikh Zaid. Egypt.

[5] Waziri, M. Yonah, Z. (2014). A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania. Advances in Computer Science: An International Journal 3: 98-106.

[6] Ziyao W, Junjie N, Z Duan, (2008). SOA core technologies and application, Publishing House of Electronics Industry, Beijing, Pp.495-497.

[7] L Lin, Yongzhao Z, Yi N. (2006) Improved RBAC model based on organization. Journal of Jiangsu University (Natural Science Edition) 27(2):147-150.

[8] Wood, C, 2005. Information Security Policies Made Easy Version 9. Information Shield, U.S.

[9] Lankhorst, M. (2005). Enterprise Architecture at Work, 1st ed, Springer, Berlin.

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 448 – 454, 2016, ISSN: - 2319-8656

Combining Neural Network and Firefly Algorithm to Predict Stock Price in Tehran exchange

Aliabdollahi
Department of Accounting
Persian Gulf International Branch
Islamic Azad Univercity,khorramshahr, Iran

Saharmotamedi
Department of Accounting
Persian Gulf International Branch
Islamic Azad Univercity,khorramshahr, Iran

Abstract In the present research, prediction of stock price index in Tehran stock exchange by using neural networks and firefly algorithm in chaotic behavior of price index stock exchange are studied. Two data sets are selected for neural network input. Various breaks of index and macro economic factors are considered as independent variables. Also, firefly algorithm is used to [redict price index in next week. The results of research show that combining neural networks and firefly optimization algorithm has better performance than neural network to predict the price index. In addition, acceptable value of error-sequre means for network error in test data show that there are chaotic mevements in behaviour of price index.

Keywords: Tehran stock exchange, neural network, firefly

1 INTRODUCTION

Investment companities are one of financial intermediaries that have role in all developed stocks of the world to create balance and discipline in stock market by purpose of increasing efficiency and investment boom. In this way, resources are effectively and efficiently are used. Hence, it's not wonderful that much researches are carried out to predict the market. A system that can determine wrinner and closer in dynamic financial market produces much interest and profit for that system [1].

Nowadays, stock investemnt is an important part of country economy. Therefore, prediction of stock price has great importance for investors to obtain the highest return from their investment. stock price index shows general position of stock market, and it helps to predict shareholders for investment [2].

The main purpose of this research is to predict stock index in Tehran stock exchange. stock price data are considered as the most important information for investors. stock prices have basically dynamic, nonlinear and non-parametric nature. It shows that investors should handle variable time series with continuous structural breaks. Therefore, not only precise prediction of stock price changes is challenging, but also investors are interested in this issue [4]. In the past, various prediction models are used. The most important models are linear regression or polynomials, average of structural models and other time series. Above models have weaknesses. It allows the researcher to consider complex and nonlinear factors affecting the prediction.

This paper is organized in three sections. In the first section, literature review is presented. The proposed algorithm is explained in the second section, The research results are presented in the third section.

2. LITERATURE REVIEW

Mazhari presented a prediction model of economic firm bankruptcy in stock by using the learner automata in 2011. This research is carried out for 200 companies from 2001 to 2009. The data results show that an equation can be presented to predict financial bunkruptcy of firms [5].

In 2012, Afsar presented in model to predict stock price by using fuzzy neural networks. In this research, the model of fuzzy neural networks is designed to predict stock price. It is computed in terms of six critera of performance evaluation. Its features are rapid convergence, high precision and strong function approximation. These researches are carried out for stock four petrochemical company of Abadan, Irankhodro, Behshahr industry development and Ghadir investment from 1999-2012. This shows that Tehran stock is almost predictable [4].

Moeinoldin presented a prediction model in 2012 to predict index of Tehran stock exchange price. This research was carried out from 2001 to 2008, and it was computed statistically, but accuracy of computations was not computed [6].

In 2014 Jusmin, in his article, predicted stock exchange in stock of stockholm, Barcelona and south korea. In this research, information of three stocks were used form 2009 to 2010 to evaluate accuracy of parameter. In figure 2-2, accuracy parameter was evaluated. Jusmin showed that fuzzy neural method was the best output [8].

Adam and his colleagues studied exchange of Persian Gulf states. The purpose of this research is to predict the price of Qatar stock, and transactions were used from 2010 to 2012. The leading neural network with 10 inputs were used. The results showed that data algorithm has higher precision to predict stock [7].

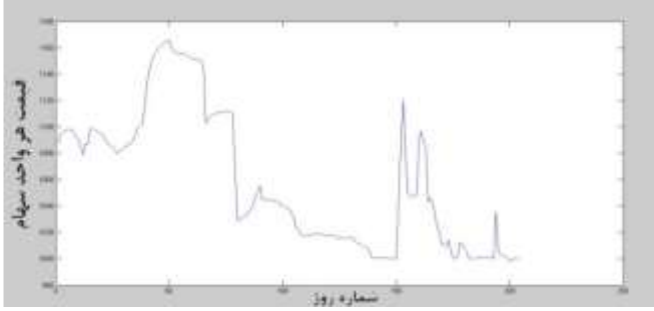
3. THE PROPOSED ALGORITHM

The problem is divided into three parts. In the first step, neural network algorithm is used, while, in the second step, firefly algorithm is used. firefly optimization algorithm is inspired from the nature, and it is proposed to solve optimization problems. This algorithm is proposed by yong in 2008 (10). This algorithm is based on food searching behavior of firefly. Minimum distance of each firefly from the aggregation of other fireflies are considered as an objective function for movement of a firefly. In firefly optimization algorithm, the movement of fireflies are formulated by the main factor: (1) movement of other creatures, 2) The behavior of searching food, 3) random distribution. In the following sections, this algorithm is precisely explained the first and second steps of this algorithm work interactively, and finally, stock equation is explained. This algorithm is implemented by Matlub.

3.1. structure of solving the problem

In order to solve the prediction problem of stock, time series are used. At first, information are gathered about a firm, and this information contains stock price in all days in one year. In figure 1, a1 example is presented

the price of each stock unit



the number of day

figure 1: information of stock price in 2012 in Saderat bank

In time seies problem, it is supposed that many changes are not observed in system behavior. Hence, it is predictable because if its behavior continuously changes, the problem is no longest predictable. Therefore, on the basis of previous information and behavior, the future of system can be estimated. This feature follows Markov approach modelling; that is, a function is extracted from the future and present behavior of system.

Generally, time-series equation is computed according to equation (1), and present time is a function of d in the past.

$$x(t) = \boldsymbol{f}(x(t-1), x(t-2), x(t-3), \dots, x(t-d))$$
(1)

In figure 2, equation (1) can be observed. It is system input of $x(t-1), x(t-2), x(t-3), \dots, x(t-d)$

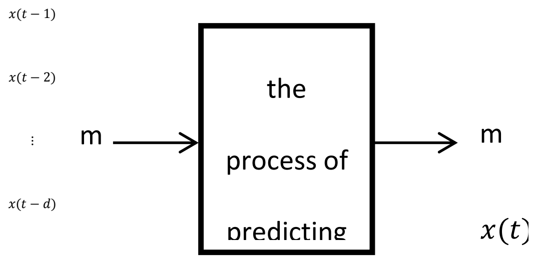


figure 2: The process of exchange prediction

It is a non-linear difference equation involving discrete time. This equation is presented in figure 3.

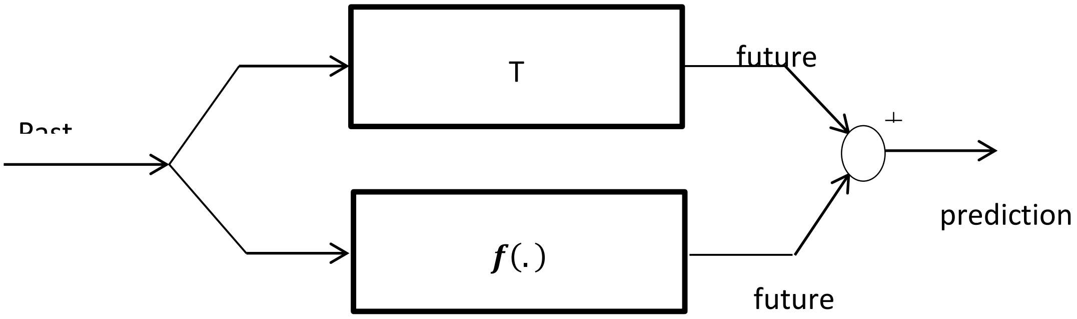


Figure 3: Comparing the process of function and stock prediction

Function should be defined in a way that prediction error is minimzed. Therefore, the prediction problem is converted to nonlinear function approximation, and it can be modelled by artificial neural network. In order to solve the problem about previous price of stock exchange, information about exchange of a firm during one year is taken into account.

Time series of stock information

If time delay (2) is considered, then equation is defined as follows.

$$x_t = f(x_{t-1}, x_{t-2}) \Longrightarrow \begin{cases} input \quad target \\ \quad x_1, x_2 \rightarrow x_3 \\ \quad x_2, x_3 \rightarrow x_4 \\ \qquad \vdots \\ x_{363}, x_{364} \rightarrow x_{365} \end{cases}$$

In the problem of predicting the stock, time delay (10) is considered (this value is computed by trial and error), and equation is considered as follows.

$x_t = f(x_{t-19}, x_{t-18}, \ldots, x_{t-10})$

$$\Rightarrow \begin{cases} input \qquad\qquad target \\ \quad x_1, x_2, \ldots, x_{10} \rightarrow x_{20} \\ \quad x_2, x_3, \ldots, x_{11} \rightarrow x_{21} \\ \qquad\qquad \vdots \\ x_{346}, x_{347}, \ldots, x_{355} \rightarrow x_{365} \end{cases}$$

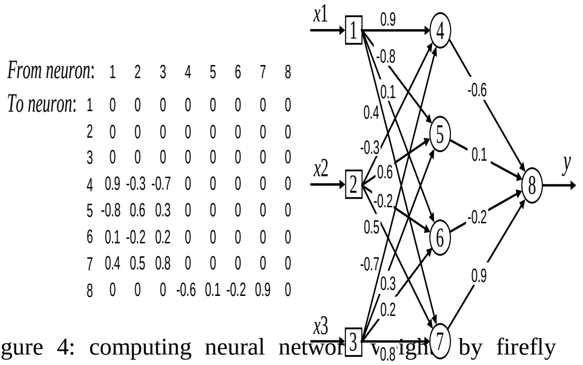
In following sections, the proposed method is investigated.

In the proposed method, the problem is divided into two parts:

1) Artificial neural network

2) Firefly algorithm

Feed forward neural network algorithm involving three layers is used for appropriate approximation (three-layers neural network is selected since it can approximate each nonlinear function). The number of neurons in middle layer is to (Value pf 10 is computed by trial and errors, then, weights value is comuted by firefly algorithm to make neural network output better. The structure of weighting is observes in figure 4). As it can be observed in figure 4, weights of neural network is located in arrays. Figure 1 presents artificial fireflies on the basis of neural network weights.



From neuron:		1	2	3	4	5	6	7	8
To neuron:	1	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0
	3	0	0	0	0	0	0	0	0
	4	0.9	-0.3	-0.7	0	0	0	0	0
	5	-0.8	0.6	0.3	0	0	0	0	0
	6	0.1	-0.2	0.2	0	0	0	0	0
	7	0.4	0.5	0.8	0	0	0	0	0
	8	0	0	0	-0.6	0.1	-0.2	0.9	0

Figure 4: computing neural network weights by firefly algorithm

Firefly :	0.9	-0.3	-0.7	-0.8	0.6	0.3	0.1	-0.2	0.2	0.4	0.5	0.8	-0.6	0.1	-0.2	0.9

table 1: The structure of artificial firefly algorithm on the basis of figure 4.

Flowchart of the proposed algorithm structure is observed in figure 5. As it can be observed in figure 5, the best output of artificial firefly algorithm determines the weight of neural network. Then, neural network is evaluated by stock data, and accuracy of neural network is considered as fitness function.

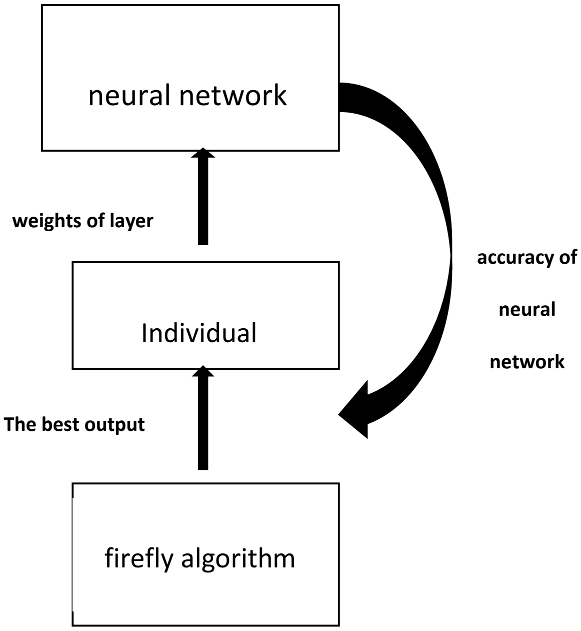


Figure 5: flowchart of the proposed algorithm structure

3.2. Algorithm parameters

The parameters of proposed firefly algorithm is observed in figure 2.

Table 2: The parameters of proposed algorithm

The value of parameter	The name of parameter
500	initial population
80	combination probability
20	mutation probability
uniform	combination type
selection algorithm	roulette wheel

4. EVALUATION OF THE PROPOSED ALGORITHM

In order to do experments window operating system in seven-core computer with processors of 5.2 GH and RAM 8G is used. For comparison, information data of twenty firms in stock gathered during one year is used.

Due to using probability-based algorithm, the program is repeated 10times to evaluated the model, and out of range data is deleted.The average of remaining data is considered as the final answer. since there many graphs, information of Behshahr food industry is only displayed with details.

4.1. Executing the algorithm of predicting the stock price for Mellat Bank

Information of Mellat Bank in 2012 involving 221 records are considered as input in firefly algorithm. Then data is divided into two test and training sets. Data test is on the basis of minimum value of time-series that is equal to 10. Among 201 inputs, 191 data are firstly selected for training, and 10 ending data are used for test.

191 data must be trained by neural network. with regard to the type of proposed algorithm, %90 of them are selevted to train the weights of neural network and %10 are selected for testing.

In table 3, two proposed algorithms are compared in terms of two criteria involving the mean of error squares and maximum profit.

Table 3: evaluating the proposed algorithm for 20 firms in stock exchange

profit percent		mean of error squares					
with optimization of firefly algorithm	without optimization of firefly algorithm	with optimization of firefly algorithm	without optimization of firefly algorithm			the name of company	row
72.78036	24.18138	0.016313	*0.003018*			Mellat Bank	1
53.77511	23.76694	0.020553	*0.008562*			Saderat Bank of Iran	2
52.17256	13.37498	0.093758	*0.005629*			oil refinery of Bandr Abbas	3
42.42715	21.01204	0.091239	*0.009169*			Iran Khodro	4
21.78661	15.26607	0.049174	*0.005682*			Azar Ab Industries	5
39.01078	33.10636	0.042241	*0.007749*			oil and gas development of Parsian	6
53.94646	44.70523	0.066753	*0.005422*			oil and gas of Tamin petrochemical	7
77.46734	25.2383	0.049019	*0.005758*			Dey Bank	8
81.84557	21.83098	0.093828	*0.004337*			oil refinery of Lavan	9
47.58577	17.50285	0.062516	*0.006479*			oil refinery of Tehran	10
84.11289	26.43155	0.084376	*0.008235*			stock of Zob Ahan Isfahan	11
29.00943	7.961876	0.055175	*0.003415*			sugar factory of Shirvan and Bojnourd	12
26.22025	12.51758	0.055589	*0.003647*			petrochemical group of Iranian	13
22.76308	11.62872	0.039502	*0.004307*			Tehran cement	14
20.46126	38.88488	0.096874	*0.005206*			Iran telecommunications	15
66.44125	40.64264	0.013337	*0.0077*			sugar factory of Naghshe Jahan	16
55.56366	9.232228	0.045607	*0.007591*			dish factory of Iran	17
42.55618	27.91901	0.057075	*0.006678*			Mihan Insurance	18
75.25859	41.8176	0.087342	*0.00723*			Sobhan Daru	19
35.098	22.59051	0.091218	*0.004866*			credit company of Askari	20

In table 3, Information of 20 firms about two criteria involving MSE and profit percent is investigated. As it can be observed, profit increases in 14 firms by using the proposed algorithm, and the profit decreases by mistake in 6 firms. Hence, it can be concluded that, by using the proposed algorithm, 70 percent of increasing profit and 30 percent of profit reduction can be observed. MSE increases considerably by adding optimization algorithm. It can be shown that the proposed algorithm involves 20-60 percent of precision.

5. CONCLUSION

In firefly algorithm, it is clear that this algorithm has higher speed in convergence of continuous problems. Also, it is specified that, by changing evlolutionary algorithm parameters dynamically, algorithm performs better. One of firefly algorithm problems is being stuck to local optimization. By using 10 percent of low population in each generatio, it doesn't face with the problem of local optimization in next generation of the algorithm.

6. REFRENCES

1. Barth, M.E., Beaver, W.H. and W.R. Landsman (2011)."The Relevance of the Value Relevance Literature for Financial Accounting Standard Setting: Another View, Journal of Accounting and Economics, 37, 77- 104.
2. Fields, T.D., Lys, T.Z., and L. Vincent (2011)."Empirical Research onAccounting Choice." Journal of Accounting and Economics, 31, 255-307.
3. Healy, P.M. and K.G. Palepu (2001)."Information Asymmetry, CorporateDisclosure and the Capital Market: A Review of the Empirical DisclosureLiterature", Journal of Accounting and Economics, 31, 405-440.
4. Holthausen, R. and R. Watts (2013)."The Relevance of the ValueRelevance Literature," Journal of Accounting and Economics, 31, 2-40.
5. Kothari, S.P. (2014)."Capital Market Research in Accounting," Journalof Accounting and Economics, 31, 105-231.
6. Lee, C.M.C, (1996)."Measuring Wealth", CA Magazine, April, 3-37.

7. Lev, B. and J.A. Ohlson, (1982)."Market-Based Empirical Research in Accounting: A Review, Interpretation, and Extension, Journal of Accounting Research" 20, 249-322.

8. Shackelford, D.A. and T.Shevlin (2014)."Empirical Tax Research in Accounting.", Journal of Accounting and Economics, 31, 321-387.

9. Stewart, B. (2015). Qust for Value, New York, Harper-Collins.

10. Gandomi, A. H., &Alavi, A. H. (2012). Krill herd: a new bio-inspired optimization algorithm. Communications in Nonlinear Science and Numerical Simulation, 17(12), 4831–4845.

International Journal of Computer Applications Technology and Research
Volume 5–Issue 7, 455-459, 2016, ISSN:2319–8656

Comparisons of QoS in VoIP over WIMAX by Varying the Voice codes and Buffer size

Nueafun Pimwong
Department of Computer Science and Engineering
Thapar University, Patiala, India

R.K. Sharma
Department of Computer Science and Engineering
Thapar University, Patiala, India

Visit Boonchom
Division of Computer and Information Technology,
Faculty of Science,
Thaksin University, Thailand

Abstract: Voice over Internet Protocol (VoIP) is developed for voice communications system based on voice packets transmitted over IP network with real-time communications of voice across networks using the Internet protocols. Quality of Service (QoS) mechanism is applied to guarantee successful voice packets transmitted over IP network with reduced delay or drop according to assigned priority of voice packets. In this paper, the goal of simulation models is present to investigate the performance of VoIP codecs and buffer size for improving quality of service (QoS) with the simulation results by using OPNET modeler version 14.5. The performance of the proposed algorithm is analyzed and compared the quality of service for VoIP. The final simulated result shows that the VoIP service performance best under G.729 voice encoder scheme and buffer size 256 Kb over WiMAX network.

Keywords: VoIP, Codecs, QoS, WiMAX, Buffer size

1. INTRODUCTION

Worldwide Interoperability for Microware Access (WiMAX) is a standard based on IEEE 802.16 broadband wireless access metropolitan area technology. It is an air-interface standard for microwave and millimeter-wave band. This server can act as a wireless extension cable and DSL technology, enabling wireless broadband access. The signal cover of WiMAX technology ups to 50km, WiMAX data rates between 1.5 to 75 Mbps. Also, it supported multimedia applications such as voice over IP (VoIP)

VoIP is developed for voice communications system based on voice packets transmitted over IP network, in possibility to reduce a communication costs. It provides real-time communications of voice across networks using the Internet protocols with Quality of Service. QoS transmitted over IP network which can reduced delay or drop according to assigned mechanism is applied to guarantee successful voice packets priority of voice packets.

In the present study, OPNET simulator is use to implement the proposed VoIP Network. We examine all the various buffer size that can drop the quality of service over wireless network (WiMAX). Accordingly to this study, it is relied on using codecs and buffer size to explore its impact on packet delay, jitter and throughput, are calculated and analyzed. The comparisons were carried out between different codecs (G.711, G.723, G.729 and GSM) and different buffer size (32kb, 64kb, 128kb and 256 kb) with are the most appropriate to improve QoS for VoIP.

This article is organized in five sections. Section 1 introduces the work. Section 2 gives the Materials and Methods for improving quality of service (QoS). Section 3 shows the results and analysis based on the modeling and simulation study. Section 4 describes the experimentation carried out in this work. Section 5 concludes the paper.

2. Materials and Methods

2.1 Quality of Service (QoS)

One can broadly divide QoS in two types: QoS for network and QoS for user. QoS for network guarantees that the packet for the voice communication shall not be delayed or dropped. A QoS for user corresponds to the degree of user satisfaction in service. These parameters are explained below:

Delay Takes place when the packets of data that contain the voice in digital form take more than estimated time in order to reach the destination. Delay can be caused by a number of factors, in factors, including, type of network, queuing discipline and type of voice packet traffic [1].

Jitter take place while transporting the voice and packet over switched network, the data may have a time variation in order to reach the destination. When some of data packets take more time in order to reach the destination the effect of this variation shall result into a jitter, for the listener at the destination [1].

Throughput Shall take place when the total received packets is given to each traffic class and measured as the mean of the number of packets produced per unit time. Throughput is inversely proportional; robust network has a lower degree of packet drop [1].

2.2 Codecs for VoIP

Codecs are the algorithm that is used to convert voice data format from analog to digital in VoIP process. In VoIP process, when a user talks using telephone or microphone, the voice format is first converted into digital format, compressed and then encoded into a predated format using codecs. Codecs is vary in the sound quality. There are many types of codecs developed and standardized by ITU-T such as G.711, G723 and G.729 for this purpose [2]. Consequently, packets are transmitted through IP network to the destination. At the destination, the digital form is converted back into the voice form.

G.711 is defined in ITU-T standard for speech codec. It delivers precise speech transmission and takes very low processor requirements. It employs pulse code modulation (PCM) or Analog-to-Digital Converter (ADC). The PCM sampling rate for the voice is 8000 frequencies per second; with a tolerance rate voice bandwidth of 4000 Hz. PCM processed samples are represented in 8 bit format, and with a high bit rate of 64 Kbps [3]. In addition, there are two versions of G.711, namely, A-law and U-law. A-law is designated for computer processing and its sample rate encode is 13 bit samples, this E1 standard is used in most of the rest of the world (other than North America and Japan). U-law is the T1 standard used in North America and Japan. Its rate encode is 14 bit samples [3]. Codec G.711 provides a higher signal range and it is the codec used by the PSTN network and is believed to be good for VoIP.

G.723 is based on the ITU-T standard that was designed for voice and multimedia communication over stand phone system. It gives high compression with high quality audio. It uses lots of processor power; these particulars are specified by the H.323 and H.324 series standards. It provides two compressed stream bit rate 5.6 Kbps and 6.3 Kbps. The higher bit rate is indicate greater quality. The code operates on speech frames of 30 ms corresponding to 240 samples at a sampling rate of 8000 voice frequencies per second [4]. It has been optimized to represent high quality speech with low bandwidth requirements using a limited amount of complexity and suitable for applications such as VoIP.

G.729 is another ITU-T standard and it has the ability to compress the payload for low bit rate by using an algorithm know as Conjugate Structure – Algebraic Code Excited Liner Predication (CS-ACELP). It gives excellent bandwidth utilization and is error tolerant. This coder offers good quality speech at a reasonably low bit rate of 8 Kbps and works on a frame of 80 speech samples [5]. It allows moderate transmission delay and is very useful in applications such as teleconferencing or visual telephony where quality, delay and bandwidth are important. Nowadays Skype is taking benefits from this standard.

GSM stands for Global System for Mobile communication this based on the codec operating with a bit rate of 13 kbps. The GSM codec provides good-quality speech. The speech input is a 16 bit word sampled at 8 KHz is analyzed by LP.

2.3 WiMAX Network

Worldwide Interoperability for Microware Access (WiMAX), is a standard based on IEEE 802.16 broadband wireless access metropolitan area technology. It is an air-interface standard for microwave and millimeter-wave band. This server can act as a wireless extension cable and DSL technology, enabling wireless broadband access. The signal cover of WiMAX technology ups to 50 km, WiMAX data rates between 1.5 to 75 Mbps. Also, it supported multimedia applications such as voice over IP (VoIP) [6]. WiMAX support its application through four distance traffic classes:

Best Effort (BE) is designed for application such as web browsing [7] that do not require QoS.

Non Real-Time polling service (nrtPS) support non real-time application such as File Transport Protocol (FTP) [7] that requires variable size of data.

Unsolicited Grant service (UGS) supports Constant Bit rate (CBR) application such as VoIP without silence suppression [8] where Base Station (BS) assigns a fixed bandwidth to users.

Real-time Polling service (rtPS) supports real-time applications with variable size data such as MPEG [8] where BS allocates bandwidth based on Subscriber Station (SS) request.

2.4 Buffer size

Buffer is memory location within router where packets are placed in queues before they get processed upon their turn [9]. The intermediate devices like router and switch in a network have buffer where the packets wait in a queue before and after processing. Depending on the packet arrival rate and the packet departure rate, which may be higher or lesser then packet departure rate, the packet size may have an impact in the percentage of discarded packets. As multiplexing increases the packet size, big packets are expected to be discarded in the bigger percentage than small ones.

3. MODELLING AND SIMULATION

3.1 OPNET Modeler

OPNET (Optimized Network Engineering Tool) is a tool to simulate the behavior and performance of VoIP network, Quality of Service (QoS) analysis of and performance of VoIP network, Quality of Service (QoS) analysis of simulator of network communication and network device and protocols. OPNET provides performance analysis of computer network and applications [10] through this we can design;

3.1.1 Simulation Model

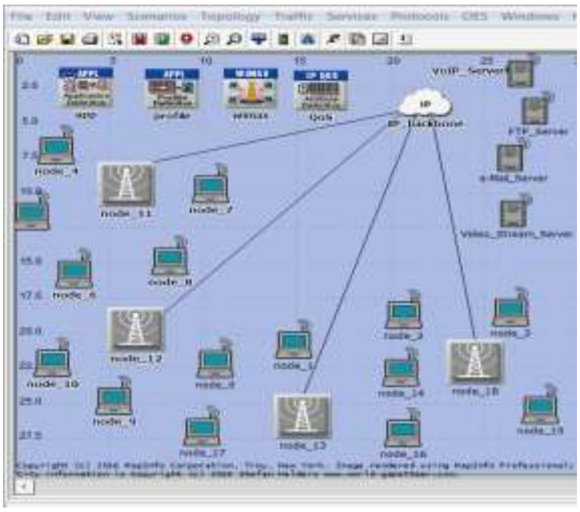


Figure. 1 The Simulation Network Model

The following figure 1 present the network model. This simulation model was run in different scenarios to determine the best audio encoding schemes and buffer size of utilizing VoIP over integrating wireless (WiMAX). All the scenarios follow the similar structure and the similar topology. Each scenario is implementing with the codec G.711, G723, G729 and GSM furthermore buffer size such as 32kb, 64kb, 128kb plus 256 kb. Various comparisons are conduced to fine the value of various parameters.

3.1.2 Simulation Parameter Setup

VoIP in Fixed WiMAX network Base Station (BS) were simulated with fifteen (15) mobile devices, where mobile devices subscriber's stations are place around each BS. All BSs were connected to the IP back bone (internet) using point-to-point protocol (PPP) without any server BS. Basic parameters associated with VoIP in WiMAX Configuration attributes, application's configuration, application profiles, task's definition, BSs and SSs for the model were configured as show in figure 1.

Table 1. Subscriber Station Parameters

Parameter	***Value***
Antenna Gain (dBi)	-1 dBi
Type of SAP	IP
Match Value	Interactive Voice (6)
Server ice das s Name	Gold
Max Transmission Power	Adaptive
PHY Pro file	0.5 W
PHY Profile Type	Wireless OFDMA 20 MHZ
Multipatch Channel Mode	OFDM
Patholoss Model	Vechicular Emifonrnaits
Terrain Type	Terrain Type A

Table 2. Base Station Parameters

Parameter	***Value***
Antenna Gain (dBi)	15 dBi
Match Value	Interactive Voice (6)
Server ice das s Name	Gold
Max Transmission Power	Adaptive
Max Transmission Power	Adaptive
PHY Profile Type	Wireless OFDMA 20 MHZ
Multipatch Channel Mode	OFDM
Multipatch Channel Mode	OFDM
Perm Has e	3

4. Simulation results and Discussion

This paper investigates the performance of WiMAX network using different quality of service (QoS) with are explained below.

4.1.1 *Quality of Service (QoS)*

Quality of Service (QoS) represents the whole performance of a WiMAX network, witness by the users of the network. To evaluation the quality of service, various related aspects of network service are often considered, for example error rates, bandwidth, throughput, load, transmission delay, availability, jitter etc.

4.1.2 *Performance Parameters*

The performance parameters are used to analyze simulation with based on the simulation results; a comparison between the effects of different codec G.711, G723, G729 and GSM as well buffer size such as 32kb, 64kb, 128kb the last 256 kb on QoS of VoIP. As stated earlier, three QoS measurements, such as voice packet end to end delay (sec), voice packet jitter (sec) and throughput (packet/sec).

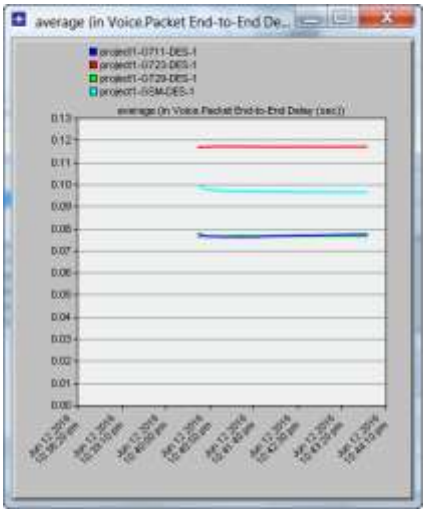


Figure. 2 Delay (sec) under various audio codes

Average end to end delay metric is show in figure 5: G711 present the best performance with respect to the other codes.

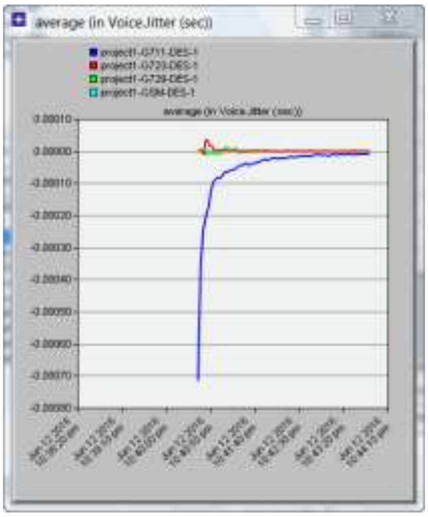


Figure. 3 Jitter (sec) under various audio codes

Figure 3 describe the average voice jitter comparison using different codecs. From graph, the jitter of G.711, G.723, G.729 and GSM increased and become very close to zero.

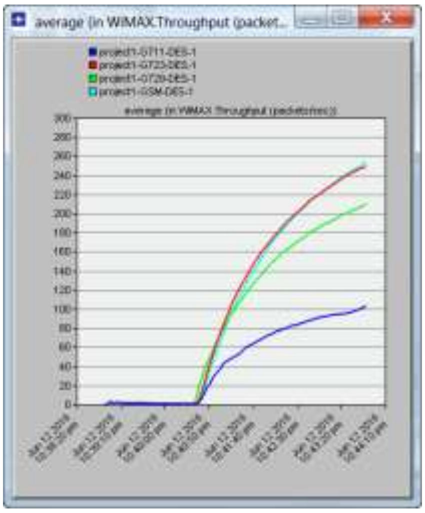


Figure. 4 Throughput (sec) under various audio codes

In figure 4, network scenarios indicated that G.729 scenario is the best in traffic send and receive in comparison with other scenarios.

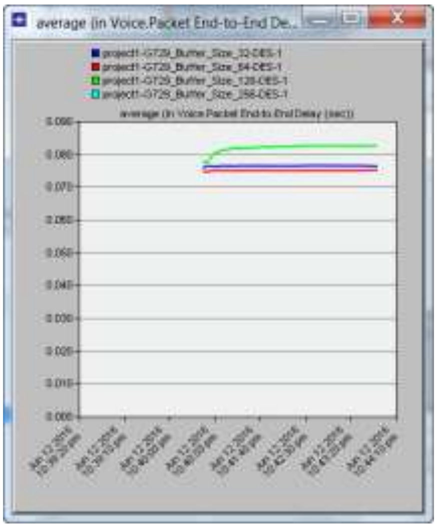


Figure. 5 Delay (sec) under various buffer size

In figure 5, it is presented in average end to end delay metric with various buffer size: 64 Kbits present the best performance with respect to the other buffer size. While high buffer size (128 kbits and 256 kbits) increased delay value.

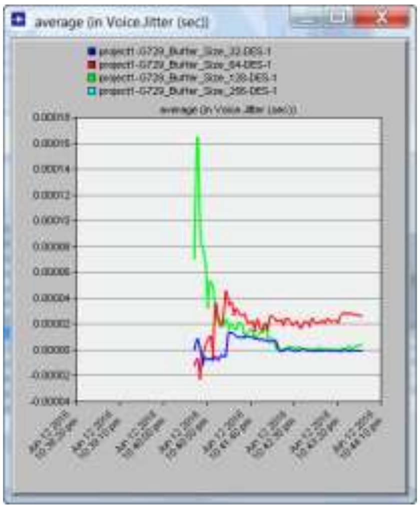


Figure. 6 Jitter (sec) under various buffer size

The performance analysis is illustrated in figure 6. The investigations present that buffer size 256 Kbits increased and become much closed to zero.

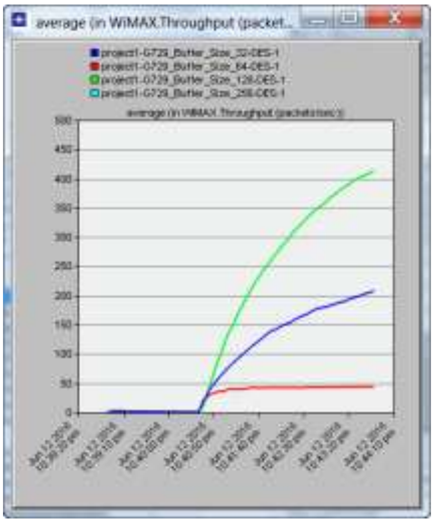


Figure. 7 (sec) under various buffer size

The simulated voice throughput in figure 7, it is observed that both 128 Kbits and 256 Kbits have same throughput at 400 (packet/sec) and this value is more than buffer size other (32 Kbits and 64Kbits).

5. CONCLUSIONS

In this paper various performance of QoS such as Jitter, Delay and Throughput, are analysed on VoIP codes and different buffer size with the help of the observation obtained from different codes and buffer size, it was found that as the no. Of buffer size increases, the value of QoS parameters (Delay and Throughput) also increases; an optimized value of QoS parameter is obtained.

6. ACKNOWLEDGMENTS

The authors are thankful to Department of Computer Science and Engineering Thapar University. Special Thanks Professor R.K. Sharma for suggestion and sweet sorghum for carrying out this project.

7. REFERENCES

[1] Eason, G., Noble, B., and Sneddon, N.I., 2008. Analysis of Quality of Service (QoS). In Proceeding of the IEEE.

[2] Kazemitabar, S., Ahmed, S., Nisar, K., and Hasballan H. B., "A Survey on Voice over IP over Wireless LANs.World Academy of Science," Journal of Engineering and Technology, 2010, in press.

[3] Ravi, R. and Kumar, V. 2008. Performance Analysis of Different Codecs in VoIP using SIP. In Proceeding of Mobile and Pervasive Computing.

[4] Ade, M., Lee, Y.C. and Kasumawait, W,. L. 2010. Performances analysis of VoIP over 802.11b and 802.11e using different CODECs. In Proceeding of IEEE.

[5] Said, B., Mohammed, B. and Anoure,. A. "VoIP over MAMET (VoMAN): QoS & Performance Analysis of Routing Protocols for Different Audio Codecs," Journal of Computer Applications, 2011, in press.

[6] Lslam, S., Rashid, M. and Tarique, M. "Performance analysis of WiMAX/WiFI system under differen codecs," Journal of Computer Applications, 2011, in press.

[7] Qureshi, A., M., Younus, A., Saeed, M., Sidiqui, A., F. Touheed, N. and Qureshi, S,. M. "Comparative study of VoIP over WiMAX and Wi-Fi." Journal of Computer Science, 2011, in press.

[8] Haghani, E. and Ansari, N. 2008. VoIP traffic scheduling in WiMAX network. In Proceeding of Global Telecommunications (GLOBECOM 2008).

[9] Malhotra, R. and Gupta, V. "Simulation & Performance Analysis of Wired and Wireless Computer Network," Journal of Computer Science and Technology, 2011, in press.

[10] Ravi R. and Kumar V. 2008. Performance Analysis of Different Codecs in VoIP using SIP. In Proceeding of Mobile and Pervasive Computing.

[11] Bagoria, N., Garhwal, A. and Shamar, A. "Simulation of Physical layer of WiMAX Network using OPNET MoDeler," Journal of P2P Network Trends and Technology (IJPTT), in press.

[12] Anouari, T. and Haqiq, A. "Performance Analysis of VoIP Traffic in WiMAX using various Service Class," Journal of Computer Application, 2012, in press.

[13] Pentikousis, K., Piri, E., Pinola, J., Fitzek, F., Nissila, T., and Harjula, I. 2008. Empirical evaluation of VoIP aggregation over a fixed WiMAX testbed. In Proceeding of Testbeds and Research infrastructures for the Development of Network & Communities.

[14] Alekande, Z., N., Bozinovski. and Janevski, T., "Performance evaluation of real-time services in mobile WiMAX", Journal of Telfor, 2010, in press.

International Journal of Computer Applications Technology and Research
Volume 5–Issue 7, 460-464, 2016, ISSN:2319–8656

Big Data Analytics: Recent Achievements and New Challenges

Dr Anand Mohan
NSHM Group of Institutions,
Durgapur-713212(West Bengal) India

Abstract : The era of Big data is being generated by everything around us at all times. Every digital process and social media exchange produces it. Systems, sensors and mobile devices transmit it. Big data is arriving from multiple sources at an alarming velocity, volume and variety. To extract meaningful value from big data, you need optimal processing power, analytics capabilities and skills. Big data has become an important issue for a large number of research areas such as data mining, machine learning, computational intelligence, information fusion, the semantic Web, and social networks. The combination of big data technologies and traditional machine learning algorithms has generated new and interesting challenges in other areas as social media and social networks. These new challenges are focused mainly on problems such as data processing, data storage, data representation, and how data can be used for pattern mining, analysing user behaviours, and visualizing and tracking data, among others. In this paper, discussion about the new concept big data and data analytic their concept, tools and methodologies that is designed to allow for efficient data mining and information sharing fusion from social media and of the new applications and frameworks that are currently appearing under the "umbrella" of the social networks, social media and big data paradigms.

Keywords - Big data, Data mining, Social media, Social networks, Social-based frameworks and applications

INTRODUCTION

Big Data is a term used to describe a massive volume of diverse data, both structured and unstructured, that is so large and fast-moving that it's difficult or impossible to process using traditional databases and software technology. In most enterprise scenarios, the data is too enormous, streaming by too quickly at unpredictable and variable speeds, and exceeds current processing capacity. According to leading technology research firm Gartner Inc., Big Data is high-volume, high-velocity, and high-variety of information assets that demand cost-effective, innovative forms of information processing for enhanced insights and decision-making. While Big Data is defined by its characteristics, the 3 "Vs" (i.e., volume, velocity, and variety), other analysts add a fourth "V" to represent the data's value. Big data is the term for a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications. The challenges that we face with DBMS tools and other technologies is capture, storage, search, sharing, transfer, analysis, and visualization.

Key enablers for the appearance and growth of 'Big-Data' are:

- Increase in storage capabilities
- Increase in processing power
- Availability of data

Globally Big Data generation in Facebook creates over 30 billion pieces of content per day and stores 30 petabytes of data and Twitter produces over 90 million tweets per day[1].

The term **"Big Data Analytics"**, when used by software vendors, refers to the technology that an organization requires to handle data at extreme scales. Not only does this make Big Data management and storage vastly different from normal or structured data that most people are accustomed to handling, but it also means that organizations now require powerful, integrated solutions for making this information usable and applicable for business analytics practices and dealing with large data sets, organizations face difficulties in being able to integrate, manipulate, and manage them efficiently and effectively.

Big Data is a huge problem in business analytics because standard tools and procedures are not designed to search and analyze massive data sets. The use of Big Data large pools of data that can be brought together and analyzed to discern patterns and make better decisions will become the basis of competition and growth for individual firms, enhancing productivity and creating significant value for the world economy by reducing waste and increasing the quality of products and services[2].

Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information. Big data can be characterized by 3Vs (volume, variety and velocity) are three defining properties or dimensions of big data. Volume refers to the amount of data, variety refers to the number of types of data and velocity refers to the speed of data processing.

According to the 3Vs (volume, variety and velocity) model, the challenges of big data management result from the expansion of all three properties, rather than just the volume alone - the sheer amount of data to be managed. The extreme volume of data, the wide variety of types of data and the velocity at which the data must be must processed. Although big data doesn't refer to any specific quantity, the term is often used when speaking about petabytes (A petabyte is a measure of memory or storage capacity and is 2 to the 50th power bytes or, in decimal, approximately a thousand terabytes) and exabytes (An exabyte (EB) is a large unit of computer data storage, two to the sixtieth power bytes. The prefix *exa* means one billion, or one quintillion, which is a decimal term. Two to the sixtieth power is actually 1,152,921,504, 606,846,976 bytes in decimal, or somewhat over a quintillion (or ten to the eighteenth power) bytes. It is common to say that an exabyte is approximately one quintillion bytes. In decimal terms, an exabyte is a billion gigabytes of data, much of which cannot be integrated easily).

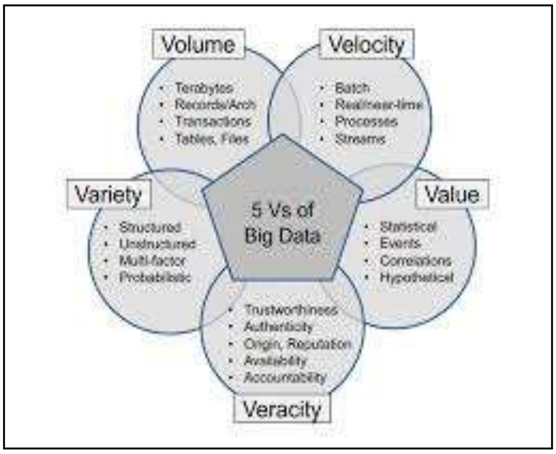


Fig 1-5Vs of Big Data

Big Data will help to create new growth opportunities and entirely new categories of companies, such as those that aggregate and analyse industry data. Many of these will be companies that sit in the middle of large information flows where data about products and services, buyers and suppliers, consumer preferences and intent can be captured and analysed. Forward-thinking leaders across sectors should begin aggressively to build their organisations' Big Data capabilities[3].

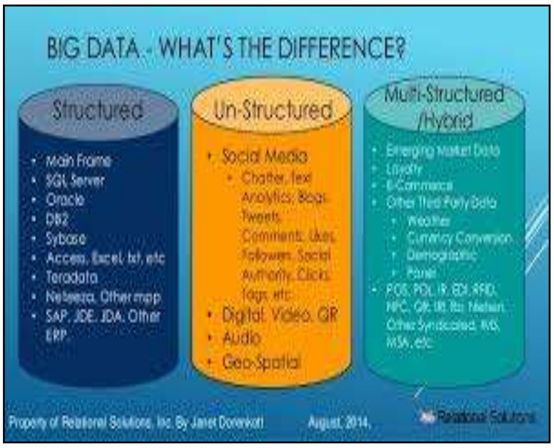


Fig 2 - Big Data Structured, Un-Structured and Multi Structured/Hybrid

Five ways to leverage Big Data are given as :

1. Big Data can unlock significant value by making information transparent. There is still a significant amount of information that is not yet captured in digital form, e.g., data that are on paper, or not made easily accessible and searchable through networks. We found that up to 25 percent of the effort in some knowledge worker workgroups consists of searching for data and then transferring them to another (sometimes virtual) location. This effort represents a significant source of inefficiency.

2. As organisations create and store more transactional data in digital form, they can collect more accurate and detailed performance information on everything from product inventories to sick days and therefore expose variability and boost performance. In fact, some leading companies are using their ability to collect and analyse big data to conduct controlled experiments to make better management decisions.

3. Big Data allows ever-narrower segmentation of customers and therefore much more precisely tailored products or services.

4. Sophisticated analytics can substantially improve decision-making, minimise risks, and unearth valuable insights that would otherwise remain hidden.

5. Big Data can be used to develop the next generation of products and services. For instance, manufacturers are using data obtained from sensors embedded in products to create innovative after-sales service offerings such as proactive maintenance to avoid failures in new products.

Big data expands the possible domains of application for algorithms and machine-mediated analysis. At some manufacturers, for example, algorithms analyze sensor data from production lines, creating self-regulating processes that cut waste, avoid costly (and sometimes dangerous) human interventions, and ultimately lift output. In advanced, “digital” oil fields, instruments constantly read data on wellhead conditions, pipelines, and mechanical systems. That information is analyzed by clusters of computers, which feed their results to real-time operations centers that adjust oil flows to optimize production and minimize downtimes. One major oil company has cut operating and staffing costs by 10 to 25 percent, while increasing production by 5 percent[4].

Computer scientists, physicists, economists, mathematicians, political scientists, bio-informatics, sociologists, and other scholars are clamouring for access to the massive quantities of information produced by and about people, things, and their interactions.

Benefits of big data analytics tools are given below :

1. Big data and big data tools offer many benefits. The main business advantages of big data generally fall into one of three categories: cost savings, competitive advantage, or new business opportunities.
2. **Cost Savings**
3. Big data tools like Hadoop allow businesses to store massive volumes of data at a much cheaper price tag than a traditional database. Companies utilizing big data tools for this benefit typically use Hadoop clusters to augment their current data warehouse, storing long-term data in Hadoop rather than expanding the data warehouse. Data is then moved from Hadoop to the traditional database for production and analysis as needed. Versatile big data tools can also function as multiple tools at once, saving organizations on the cost of needing to purchase more tools for the same tasks.
4. **Competitive Advantage**
5. New Business Opportunities
6. The final benefit of big data analytics tools is the possibility of exploring new business opportunities. Entrepreneurs have taken advantage of big data technology to offer new services in AdTech and MarketingTech. Mature companies can also take advantage of the data they collect to offer add-on services or to create new product segments that offer additional value to their current customers. In addition to those benefits, big data analytics can pinpoint new or potential audiences that have yet to be tapped by the enterprise. Finding whole new customer segments can lead to tremendous new value.
7. These are just a few of the actionable insights made possible by available big data analytics tools. Whether an organization is looking to boost sales and marketing results, uncover new revenue opportunities, improve customer service, optimize operational efficiency, reduce risk, improve security, or drive other business results, big data insights can help[5].

The use cases for big data analysis are given below :

1. Big data analytics lends itself well to a large variety of use cases spread across multiple industries. Financial institutions can quickly find that big data analysis is adept at identifying fraud before it becomes widespread, preventing further damage. Governments have turned to big data analytics to increase their security and combat outside cyber threats. The healthcare industry uses big data to improve patient care and discover better ways to manage resources and personnel. Telecommunications companies and others utilize big data analytics to prevent customer churn while also planning the best ways to optimize new and existing wireless networks. Marketers have quite a few ways they can use big data. One involves sentiment analysis, where marketers can collect data on how customers feel about certain products and services by analyzing what consumers post on social media sites like Facebook and Twitter.
2. The number of use cases are plentiful, and no industry should think that analytics couldn’t be used in some way to improve their businesses. That type of versatility is part of what has made big data so popular. And these are only a few examples of use cases. As companies and other organizations become more familiar with all of the capabilities granted through big data analytics, more use cases will likely be discovered, adding to big data’s overall value. As with any developing technology, the process may take some time, but eventually its widespread use will lead to the discovery of even more benefits and uses.

Some of the Top Big Data Tools overview:

1. **Apache Hadoop :**Hadoop is an open source software framework originally developed by Doug Cutting and Mike Cafarella in 2006. It was specifically built to handle very large data sets. Hadoop is made up of two main parts: the Hadoop Distributed File System (HDFS) and MapReduce. HDFS is the storage component of Hadoop. Hadoop stores data by splitting files into large blocks and distributing it across nodes. MapReduce is the processing engine of Hadoop.

Hadoop processes data by delivering code to nodes to process in parallel.

2. **Apache Spark :**Apache Spark is quickly growing as a data analytics tool. It is an open source framework for cluster computing. Spark is frequently used as an alternate to Hadoop's MapReduce because it is able to analyze data up to 100 times faster for certain applications. Common use cases for Apache Spark include streaming data, machine learning and interactive analysis.

3. **Apache Hive :**Apache Hive is a SQL-on-Hadoop data processing engine. Apache Hive excels at batch processing of ETL jobs and SQL queries. Hive utilizes a query language called HiveQL. HiveQL is based on SQL, but does not strictly follow the SQL-92 standard.

4. **NoSQL Databases :** NoSQL databases have grown in popularity. These Not Only SQL databases are not bound by traditional schema models allowing them to collect unstructured datasets. The flexibility of NoSQL databases like MongoDB, Cassandra, and HBase make them a popular option for big data analytics[6].

Big data in the cloud - Big data analytics can be a complex concept, one that many businesses may feel like they're not ready for. Big data infrastructure can get to be complicated, and without the right personnel on hand, maintaining it can be a monumental task. One solution to this significant problem is for companies to head to the cloud for their big data needs. Many cloud vendors already provide a variety of services through the cloud, and big data analytics is just the latest example of this. Taking big data to the cloud offers up a number of advantages. Improvements come in the form of better performance, targeted cloud optimizations, more reliability, and greater value. Big data in the cloud gives businesses the type of organizational scale many are searching for. This allows many users, sometimes in the hundreds, to query data while only being overseen by a single administrator. That means little supervision is required.

Big data in the cloud also allows organizations to scale quickly and easily. This scaling is done according to the customer's workload. If more clusters are needed, the cloud can give them the extra boost. During times of less activity, everything can be scaled down. This added flexibility is particularly valuable for companies that experience varying peak times. Big data in the cloud also takes advantage of the benefits of cloud infrastructure, whether they be from Amazon Web Services, Microsoft Azure, Google Cloud Platform, or others.

Gathering data from various sources is, of course, only one part of the big data analytics process. All that data needs to be stored somewhere, and that repository is often referred to as a **data lake**. Data lakes are where data is kept in its raw form, before any organizational structure is used and before any analytics are performed. Data lakes don't use the traditional structure of files or folders but rather use a flat architecture where each element has its own identifier, making it easy to find when queried. Data lakes are a type of object storage that Hadoop uses, making it an effective way to describe where Hadoop-supported platforms pull their data from. One major benefit of having a data lake is the ability to store massive amounts of data. As big data continues to grow, the need for that near limitless storage capability has grown with it. Data lakes also allow for added processing power while also providing the ability to handle numerous jobs at the same time. These are all capabilities that have been increasingly in demand as more enterprises use big data analytics tools.

Many different types of solutions are required to support the wide range of big data use cases. From simple spreadsheets to advanced analytics and marketing solutions to analytics engines, Qubole provides effortless integration to centrally analyze your data all in one spot.

Spreadsheets and Analytics Tools: Through ODBC connectors, Qubole customers can connect to Microsoft Excel and tools from leading analytics vendors such as Tableau, Qlik, MicroStrategy, and TIBCO Jaspersoft. In addition, the R statistical programming language can be integrated with Qubole using ODBC/REST APIs.

Analytics Engines: Qubole offers connectors for massively parallel processing databases such as Vertica as well as relational database engines such as Microsoft SQL Server and the MySQL open source database, and NoSQL databases such as MongoDB[7].

CRM and Online Marketing Solutions: Qubole also connects to leading CRM and online marketing platforms such as Salesforce.com and online marketing and web analytics solutions such as Omniture and Google Analytics.

CONCLUSION

The era of Big Data could yield new management principles. In the early days of professionalized corporate management, leaders discovered that minimum efficient scale was a key determinant of competitive success. Likewise, future competitive benefits are likely to accrue to companies that can not only capture more and better data but also use that data effectively at scale. Companies have decided that big data is not just a buzzword, but a new fact of business life -- one that requires having strategies in place for managing large volumes of both structured and unstructured data and with the reality of big data comes the challenge of analyzing it in a way that brings real business value. Business and IT leaders who started by addressing big data management issues are now looking to use big data analytics to identify trends, detect patterns and glean other valuable findings from the sea of information available to them. Big data analytics technologies on their own aren't sufficient to handle the task. Well-planned analytical processes and people with the talent and skills needed to leverage the technologies are essential to carry out an effective big data analytics initiative. The information resources collected here to learn about big data analytics best practices from experienced users and industry analysts -- from identifying business goals to selecting the best big data analytics tools for organization's needs.

REFERENCES

[1]. http://searchcloudcomputing.techtarget. com
[2].https://www.qubole.com/resources/articles/big-data-analytics/?nabe= 5695374637924352:1&utm_referrer=https%3A%2F%2Fwww.google.co.in#sthash.UL6ZrfK9.dpuf
[3].http://searchbusinessanalytics.techtarget.com/essentialguide/Guide-to-big-data-analytics-tools-trends-and-best-practices
[4].http://www.infoworld.com/article/2616959/big-data/7-top-tools-for-taming-big-data.html
[5].http://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/
[6].http://www.in.techradar.com/news/world-of-tech/The-importance-of-big-data-analytics-in-business/articleshow/44104837.cms
[7].http://datascienceseries.com/stories/ten-practical-big-data-benefits

International Journal of Computer Applications Technology and Research
Volume 5– Issue 7, 465 - 471, 2016, ISSN:- 2319–8656

Suitability of Agile Methods for Safety-Critical Systems Development: A Survey of Literature

Mary Walowe Mwadulo
Department of Information Technology
Meru University of Science and Technology
P.O BOX 972-60200 Meru, Kenya.

Abstract: Lately, agile methods have widely been used in large organizations. This contrasts to previous practice, where they were mainly used for small projects. However, developers of safety critical systems have shied away from using these methods for the right and wrong reasons. Adoption of agile methods for safety critical system development is low and there is need to find out why this is so especially since agile methods allow a more relaxed approach towards documentation, flexible development lifecycle based on short iterations and accommodates changing requirements. This paper presents a report of a detailed analysis of literature and aims to shed light on the suitability of agile methods for developing safety critical systems .The findings indicate that many organizations are relying on traditional methods to develop safety critical systems because they are familiar with them and have been thoroughly tested over time. However with the advent of agile methods there is a paradigm shift by non safety critical system developers, nevertheless this is not happening with the safety critical system developers and there is need to find out why.

Keywords: Agile methods, agile methodology, safety-critical systems, Suitability

1. INTRODUCTION

A safety critical system sometimes referred to as life critical system is a system whose failure or malfunction can cause harm or is responsible for preventing harm [1]. The high costs of failure of safety critical systems means that trusted methods and techniques must be used for development. Consequently, safety critical systems are usually developed using well-tried techniques rather than embrace new techniques and methods such as agile. [2],[3] indicate that about 80% of respondent organizations were following an agile approach because researchers and practitioners wanted a method which would replace the bureaucratic traditional methods. This sharply contrasts to previous practice where agile methods were used for small organizations developing small applications. The interpretation of the word agile methods varies from one researcher to another. In [4] it is an umbrella for well defined methods which also vary in practice. Notably, Safety critical system developers have shied away from applying agile methods and very little rigorous research existing in this area [2]. Developers have continued to apply traditional methods such as Waterfall, V-model and Iterative and Incremental approach [1], [5].

Adoption of agile method for safety critical system development is low. In [5] only 25% of organizations develop software in accordance with agile practices, thus there is need to find out why this is so especially because agile methods allow a more relaxed approach towards documentation, flexible development lifecycle based on short iterations and accommodates changing requirements which are a great concern for the traditional methods.

The paper aims to shed light on suitability of agile methods for developing safety critical system.

In [1] agile methods will be suitable for safety critical systems when they are tailored and customized to ensure that safety objectives are met. However, there is limited support for developing safety critical software because quality control mechanisms supported by current agile processes have not proven to be adequate to assure users that the product is safe. Also, agile practices such as code refactoring, minimal documentation, iterative development, conservative nature of critical systems developers and not wanting to make internal operations public have been identified to be unsuitable for safety critical systems development and have deter agile adoption [1], [5].

The remaining part of this paper is structured as follows: section 2 presents safety critical systems, section 3 presents agile methods, section 4 presents the discussion and section 5 presents conclusion.

2. SAFETY CRITICAL SYSTEMS

The main concern with safety critical systems is the consequence of failure. If the failure of a system could lead to consequences that are determined to be unacceptable, then the system is safety-critical. In essence, a system is safety-critical when we depend on it for our well being. An example of safety-critical system failure which was reported by Ben-ari M. is Ariane V launch failure caused by a software error. As such, safety critical systems must be certified by a regulatory agency to ensure that they are fit-for-purpose. This ensures proper development practices have been applied to promote system correctness as the final outcome. It is important that adherence to the objectives of the relevant standards can be demonstrated [1]. These standards identify the objectives that a system or project must meet before it is allowed to be deployed in its operational environment. Because it is virtually impossible to demonstrate deterministic correctness for any significant piece of software, most of these standards have concentrated on specifying process objectives and requirements for evidence that the processes have been followed [1]. Some of the standards include: DO-178C (Software Considerations in Airborne Systems and Equipment Certification), DO-331 (Model-Based Development and Verification) and DO-332 (Object Oriented Technology and Related Techniques). Although these standards specify the objectives that any process must meet if it is used to develop a safety-critical system, the standards do not specify the processes themselves [1]. As long as a process can be demonstrated to meet the needs of the relevant standard, the development team is free to use whatever processes they desire. This leaves the option available to use agile methods, with their accompanying advantages, provided that the safety objectives can be achieved.

In [1],[5] 50% of the organizations are developing software in accordance with the V-Model, 25% in accordance with agile practices and remaining 25% in accordance with other development lifecycles such as the Waterfall, and Iterative & Incremental approaches. This implies 75% of organizations are using traditional methods which involve huge effort in planning and documenting yet little time is spent in actual development. A lot of time is spent in early planning, more than is justifiable given that little information is available at initial stages of a project. Agile holds that this work should be done in a way that discovers and repairs defects immediately so that the emphasis is on defect avoidance in the product itself, rather than production of documentation.

3. AGILE METHODS

Agile methods were introduced as an alternative to traditional methodologies, which had a lot of documentation and were too restrictive when dealing with changing requirements. In response to these concerns agile methods offer a more relaxed approach towards documentation and provide a flexible development lifecycle based on short iterations.

Plan-driven methodologies have proven to be valuable and useful in safety critical projects, the evolving market of software products of the last few years puts this approach to the test. A growing competition, ever changing technologies and more diverse groups of clients have changed the expectations towards software development methods [3]. The need to deliver systems of acceptable quality, faster and at lower cost in comparison to competitors evoked seeking an alternative.

Table 1: Summarized comparative study of the different agile methodologies:

No.	Agile Methodology	Team size	Iteration Length	Support distributed team	System Criticality	Application area
1	Extreme Programming (XP)	Small to medium size	2-3 Weeks	No	Not geared for one system	Projects that require 2 -10 programmers
2	SCRUM	7-10 people	4 Weeks	Yes	Not Addressed	Software and non software projects
3	Feature Driven Development (FDD)	4- 20 people	1 – 4 Weeks	Yes	Not addressed	Large complex banking projects
4	Dynamic Software Development Methodology (DSDM)	2-6 People	Not addressed	Not addressed	Not addressed	Used in Europe
5	Adaptive Software Development	Determined by scope and size of the project	Determined by project schedule and the degree of uncertainty	Yes	Addresses: Risk analysis and aversion techniques	Has not be used as a methodology to develop a system
6	Crystal methodologies	Any team size, highly skilled and experienced	4 Months for large, highly critical projects	Yes	Addresses: Failure resulting in loss of money and life	Used in internet banking
7	Agile Modelling (AM)	Depends on the development process being used	Depends on the development process being used	Depends on development process being used	Depends on the development process being used	No record of current or previous use of the methodology

3.1 Agile methods used for developing safety critical systems

Several agile methods exist, but Extreme programming and SCRUM have been applied in the development of safety critical systems.

3.1.1 Extreme Programming (XP)

Extreme Programming targeted small co-located teams developing non critical products. It guides the developer through planning, coding, designing and testing phases. The purpose is to deliver what the customer needs at the time it is needed, emphasize on team work and accept changes anytime [6]. XP is suitable when requirements are unclear or dynamic and the project has high risks. However, it is unsuitable when the team is large, low cooperation between the developer and the customer and testability is not done throughout the project.

In [7] used a select number of XP practices during the development of safety critical systems and reported to have had a 53% improvement in average quality compared to the plan-driven software development projects.In [8] describes how XP practices are used in a large company developing safety critical system. He suggests that some XP practices, such as simple designs integrated with test first development and refactoring work quite well in the safety critical area.

3.1.2 SCRUM

SCRUM methodology was initiated by Ken Swaber in 1995 [6]. It has project management as part of its practices with the aim of simplifying project control through simple processes. The team does not move to a new phase unless the current one is complete. It is not suited for products where the focus is on usability [6].

In [9] presented a novel idea to integrate SCRUM into safety cycle to enable iterative incremental development in safety critical systems.

3.2 Merits of using agile methods for safety critical systems development

Agile methods have a reputation for being fast and adaptive but undisciplined and lacking in robustness. However, agile methods require a great deal of discipline, and these practices enhance both quality and team productivity. Because of this, agile development practices should be applied to the development of safety-critical systems.

Douglass [1] identified secondary benefits to using agile methods which include improved productivity, improved time to market, improved customer satisfaction and decreased development costs.. This is achieved by getting the development right the first time, and by doing things in such a way that you can verify them as you are doing them.

Verifiable artifacts can be incrementally created using agile methods which makes analysis, simulation and testing easy. The construction and verification of components during system development is a key benefit that agile brings; this iterative process offers the sort of quality improvement needed in safety-critical systems at a (relatively) low price.

Vouri [10] analyzed general agile values, principles and practices against general principles of safety-critical software development and concluded that many features of agile development can be beneficial for creating truly safe systems. He identified incremental release, reduced documentation and increased customer participation as some of the benefits of agile methods. In [11] identified benefits such as early return on investment, short time to market, improved quality, enhanced client relationships and better team morale.

3.3 Demerits of using agile Method for critical system development

There is some doubt that agile methods alone cannot be sufficient to handle development of safety critical systems .The quality control mechanisms supported by current agile processes have not proven to be adequate to assure users that the product is safe

Agile practice of having minimal documentation would have a detrimental impact on the development of safety critical systems because it is crucial to ensure traceability. Traceability helps to establish compliance to standards and regulations [2]. McHugh [5] attempted to solve the traceability issue by suggesting a tool “echo” that provides a mechanism to maintain traceability between the requirements and each stage of development while developing software in accordance with agile practices. However, [1], [2] suggested adding traceability links. Links are automatically established as developers check in code that implements a certain task.

Refactoring is another agile practice that would not fit naturally with the development of safety critical systems. If code is refactored on a critical system, it has the potential to invalidate previous certification or security analysis. This would cause extensive rework and would need to be avoided, whenever possible.

For safety critical system development there is need to have up front planning so that certification and safety analysis can be carried out early in the project. However, up-front planning can be difficult to perform following agile practices as requirements are volatile changes are welcomed and expected in an agile project. McHugh [5] has recommended before a project begins agile practices it can use techniques such as user stories.

Iteration is an agile practice that allows a project to be released in piecemeal which helps handle complexity. These iterative, incremental ways of working are significantly better at producing software with fewer defects in less time than serial waterfall approaches [1]. However, regulatory standards prohibit developers from releasing software to a live environment without been fully tested [1].

3.4 Adopting agile methods for safety- critical systems

There is a growing body of evidence supporting the theory that incorporating agile practices into safety-critical projects is not only feasible but also potentially profitable. Lukasiewicz [3] made a literature survey on applying agile methods in regulated environments and found only a small number of publications which, they think “could indicate a very low level of adoption of agile methods in regulated safety critical domain; however it may indicate a reluctance of companies in these domains to make their internal practices public”. In their paper, they reported some issues with agile methods and suggested solutions to make agile work.

Paige [12] studied agile in the development of high-integrity systems, including the analysis of elements in agile and the adaption of agile processes. Their main finding was that agile methods can be adapted to safety-critical development by not replacing plan driven processes, but applying them in appropriate tasks.

Gary [13] suggested agile methods are suitable for open source safety critical software, because these methods are synergistic with safety principles, not orthogonal to them. Agile methods bring strong practices in the area of process management and software construction, while having a philosophy that allows for traditional safety-oriented practices to the extent they are warranted. This reinforces Boehm [14] argument comprehensive project management is required for safety-critical software development.

In [15] analyzed application of agile methods in aerospace industry, however there results cannot be generalized due to specific requirement in aerospace development. They concluded that agile methods can be applied but more cooperation is needed within the aerospace community.

In [16] presented an approach on how incremental methods can be used in safety critical development. They claimed that agile methods can provide benefits, but the methods are not directly applicable in regulated areas. They suggested an upfront design in the process that at least produces information for a hazard analysis, before the agile portion of the process begins. The iterations of the software that the agile process produces also needs to include sufficient arguments that the software releases are sufficiently safe. For large scale development they propose a modular system where the modules are dependent on each other by arguments.

Pikkaraine [17] found that Agile Assessment is an efficient method to clarify what agile practices are suitable for the organization’s product development and customer co-operation. Another finding was that the use of the best suitable agile practices would improve incremental development monitoring and traceability of requirements.

Douglass [1] discussed six steps to successful agile adoption which correlates with Sidky [11] three main stages. They agree, there is need to know what makes the agile software suitable for them.

4. DISCUSSIONS

In this review I presented what is currently known on using agile methods for developing safety critical systems. Results show that there has been little research in this area and the research available is subjective with no empirical evidence to support the findings. Most studies conducted were based on case studies with no rigorous controlled experiments. Therefore, it seems that evidence on determining suitability of agile methods for safety critical systems development needs more research.

Researchers attempted to determine suitability through identification of agile practices or developing framework that points out how agility should be handled. Sidky [11] looked at suitability in terms of agile practices. They discussed three stages (Making the Go/No-go decision, discarding inappropriate practices and determining the right practices to adopt) that will enhance applicability of agile practices to mission and life critical systems. They recommended that minimal documentation and evolvability of requirements is unsuitable for safety critical systems although it is emphasized a lot in agile software development. McHugh [5] agrees in addition to regulatory compliance, lack of upfront planning and the process of managing multiple releases. He makes recommendation on how these barriers can be overcome and points out a research gap in identification of critical success factors for using agile practices when developing medical device software.

Lukasiewicz [3] discussed risks posed by introducing agile practices to safety critical software's. He concluded that agile methodologies should be regarded as complementary to plan driven practices instead of being the replacement. However, his point of view was from a software engineer perspective and the research was not conclusive since the data collected during the experiment was not yet finally processed. Therefore what was presented reported on the scope of the raw data collected than the final conclusion derived from the data.

Vuori [10] analyzed the agile principles and processes and gave guidance on how organizations could change their processes to a more agile way without risking the safety or marketability of the products or causing increased product and liability risks. However the unanswered question how an organization will know it needs to be agile

Djik[18] designed frameworks which help software practioners determine whether a software project is suitable for an agile method. He discussed two contingency factors; influence of limitation of agile methods and organization capability to handle agility which is determined by the culture values of the organization and the individual capabilities of the team. However suitability is not a term which is expressed in observable, quantifiable factors, but rather a scale where complete suitability only exist in an ideal situation. Then the big question is how to measure suitability? Yet there is no empirical research that has been conducted which links observable values of contingency factors to methodology selection. Though he concluded the model was suitable for the particular environment, the model was not validated. In [9] proposed a novel idea for developing safety-critical software-intensive systems by the use of Scrum into the safety lifecycle to enable iterative incremental development in safety-critical systems. While these models of adapting agile practices to suit safety-critical projects are valuable sources of knowledge, there is still a need to develop a more easy to use and thorough set of guidelines for safety-critical software companies that would like to adapt agile practices into their project development.

Attempts made to replace traditional methods with agile methods fail and [3] suggested that agile methodologies should be regarded as complementary to plan driven practices instead of being the replacement.

5. CONCLUSIONS

The low adoption of agile methods for safety critical systems development is as a result of developers of these systems being too conservative and wanting to use the traditional methods because they have been tested and they are familiar with. This cannot be entirely blamed on them given the fact that the consequence of failure of such systems can be catastrophic. There is also the reason of an organization not wanting to make its internal operations public and as such would want to use a method that they already know. Also agile practices such as minimal documentation, refactoring of code, upfront planning and iterative release of project contradicts safety requirement standards of safety critical systems. However, agile methods can help improve both quality and productivity and can be employed in the development of safety-critical systems. In safety-critical development, the key concern is safety, and in agile methods, the paramount concern is quality thus, there is no contradiction. Success stories of using Extreme programming and SCRUM agile methods have been documented though most of them were based on case studies. Safety-critical systems are difficult to develop. In addition to normal concerns about quality and time-to-market, safety critical systems must also meet the demanding objectives of relevant safety standards and are subject to rigorous certification. However, if an agile method is chosen carefully, the benefits would be tangible and, despite the concerns, actually increase the chance of developing a stable safety critical system. Importantly, agile practices should be tailored to the needs of safety-critical systems development.

6. REFERENCES

[1] Douglass, B.P., and Ekas, L.. Adopting agile methods for safety-critical systems development. IBM, 2012. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=RAW14313USEN

[2] Fitzgerald B and Stol K. and Sullivan R. and Donal O. Scaling agile methods to regulated environments: An industry case study, 2013.

[3] Lukasiewicz K. assessment of risks introduced to safety critical software by agile practice: a software engineer's perspective, 2012.

[4] Pathak K. and Saha A. , 2013. Review of agile software development methodologies

[5] McHugh M. Integrating Agile Practices with a Medical Device Software Development Lifecycle, 2012.

[6] Hneif M. and Ow S. Review of agile methodologies in software development. International Journal of Research and Reviews in Applied Sciences, 2009.

[7] Drobka,. Piloting XP on Four Mission-Critical Projects. IEEE Software, 2004.

[8] Greening, J. Launching XP at a Process-Intensive Company. IEEE Software, 2001.

[9] Guo Z. and Hirschmann . An Integrated Process for Developing Safety-critical Systems using Agile Development Methods, 2012.

[10] Vouri M. Agile development of safety critical software, 2011.

[11] Sidky, A. and Arthur, J. Determining the applicability of agile practices to mission and life-critical systems. In *Proceedings of the 31st IEEE Software Engineering Workshop*, SEW '07, pages 3–12, Washington, DC, USA. IEEE Computer Society,2007.

[12] Paige R. et al Towards Agile Engineering of High-Integrity Systems. Proc. of 27th International Conference on Computer Safety, Reliability and Security (SAFECOMP) 2008.

[13] Gary et al. Agile methods for open source safety critical software, 2012.

[14] Boehm B. Get ready for agile methods with care.,2002.

[15] VanderLeest and Butler (2009)

[16] Ge, X., Paige, R. F., and McDermid, J. A. (2010). An iterative approach for development of safety-critical software and safety arguments. In *Proceedings of the 2010 Agile Conference*, AGILE '10, pages 35–43, Washington, DC, USA. IEEE Computer Society.

[17] Pikkarainen M.An approach for assessing suitability of agile solutions: A case study, 2005.

[18] Djik V. Determining the suitability of agile methods for a software project, 2011.

Data Mining: Investment risk in the bank

Ali Abdolahi
Sama Technical and Vocational Training College
Islamic Azad University, Mahshahr Branch
Mahshar,Iran

Mohammad Farzizadeh
Sama Technical and Vocational Training College
Islamic Azad University, Mahshahr Branch
Mahshar,Iran

Abstract: This paper will discuss the technology and methods behind data mining, how data mining works, how it helps to improve national security, and how sustainable the technology is. Sustainability, with regard to data mining, refers to the impact on the quality of life. Quality of life refers to the preservation of human rights and the ability to feel secure. The ethics and the fallbacks regarding privacy will also be discussed in depth, including the benefits that accompany these fallbacks, and whether they outweigh the cons. Both technical and ethical articles will be used to highlight and discuss the potential, good and bad, and the controversy of data mining. Applications of data mining to security will also be proposed.

Data mining methods are expanding rapidly allowing for the mass collection of information. This mass amount of information is then used by many government agencies to identify threats, gain intelligence, and obtain a better understanding of enemy networks. However, the ability to collect this information from any computer draws into question whether or not data mining leads to a violation of the average citizen's privacy and has created a debate as to if data mining is ethically plausible.

Keywords: Classes, Clustering, Data Mining, Neighborhoods, Networks and Rules, Security, Sustainability

1. INTRODUCTION

Within the past 5 years, data mining has become more and more prevalent in the United States due to recent scandals and exposes on the topic. Simply put by Jason Frand, a professor of computer technology, data mining "is the process of analyzing data from different perspectives and summarizing it into useful information" [1]. Due to major advances in technology and the average person's growing dependence on technology, data mining now affects almost every citizen in the United States, whether he or she is aware of it or not. Within the past ten years, data mining has become an essential tool that government organizations, such as the National Security Agency and the Central Intelligence Agency, use to protect the country and gain intelligence on potential threats.

Inside data mining there are several techniques, both old and new, referred to as clustering, classification, neighborhoods, decision trees, and neural networks. Each of these techniques utilizes algorithms to find connections and trends in people's everyday computer recorded activity [2]. This allows the government to identify potential threats within the country and outside of the country. However, in order to effectively data mine the government needs mass amounts of information from every citizen's computer activity. This leads to the fear that if the U.S. government has access to every citizen's computer activity, the government could have access to personal files and documents, which many could argue violates the rights of citizens [3]. Owing to the large amount of people data mining impacts, it could have a major effect on the quality of life of future generations. This draws into question how sustainable, in terms of quality of life, data mining is. Quality of life pertains to the retention of human rights and the ability to feel secure. Despite this, data mining is a continuous innovation [1]. It is constantly growing and changing as the technology the world uses grows and changes. New techniques and uses are frequently discovered; however, its most useful application is security, despite the controversy it generates.

2. TYPES OF DATA MINING

The subject of data mining is full of many complex techniques. Within data mining are two main classifications: classical data mining and next generational data mining [2]. Clustering, classification, and trees are all considered classical techniques, while the neighborhoods technique is considered next generational. Many of these techniques are combined, or build off of one another, to more efficiently data mine. In order to understand the more complex techniques and their potential, one must first understand the basics, or the building blocks

2.1 Clustering

Clustering, to put it simply, is the grouping of like things [2]. It is a building block technique that is often needed to use more complex data mining methods. This method can be used to sort and group numbers, topics, key words and anything else one may find useful. Within clustering there are two subcategories, hierarchical and non-hierarchical.

A hierarchical cluster starts with the broadest topic and breaks that topic into smaller groups or clusters, like shown in Figure 1. Hierarchical clusters are easier to understand and allow the analyst to define how many clusters are created, unlike their non-hierarchical counterpart [2]. A non-hierarchical cluster does not create this hierarchy, rather it just creates various clusters of data. Within non-hierarchical clustering are two other subcategories of methods referred to as single-pass methods and reallocation methods [2]. Reallocation methods move data from one cluster to another in order to better organize data within the clusters. The single pass method simply runs through the data once which results in less specific clusters [2].

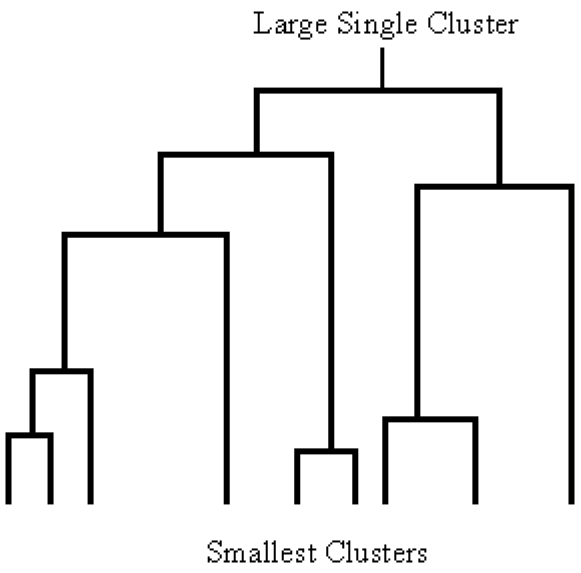


FIGURE 1 Above is a diagram of a hierarchy of clusters. The largest cluster is split up into smaller and smaller groups[2]

In order to choose which clustering method to use, one may consider how efficiently or timely he or she needs to organize the data and how specific the sorting needs to be. Non-hierarchical methods are quicker at sorting data than hierarchical methods, however, clusters are not broken down into more specific categories [2]. Data can be sorted even more quickly depending on which non-hierarchical method an analyst picks. Reallocating data requires more computer power and time than using a single-pass method. Therefore, specificity and efficiency are two factors to be taken into account when considering various methods of clustering. Specificity can be enhanced with classification, another method of data mining.

2.2 Classification

Classification, or classes, is a technique that stores data in order to locate different data in predetermined groups or classes, which will tell you more than the previously stored data alone [1]. This technique can be used in two ways, to build an archetype of an item, a product, or anything else one may find useful, or it can be used to add to other types of data mining such as trees and clustering [4]. For instance, attributes from different classes can be used to enhance clustering, specifically by using these attributes to find clusters [4].

In order to apply classification to security, a classification algorithm could sort through data and categorize potential threats based off people's age, criminal history, personal affiliations, etc. The algorithm would be categorizing based off of the known archetype of someone who, in the future, would pose a threat. This would allow organizations such as the Central Intelligence Agency or the National Security Agency to profile potential threats and possibly stop future attacks or security breaches. Classification and clustering are able to lead into another technique for data mining, neighborhoods.

2.2.1 Neighborhoods

According to Professor Jason Frand of UCLA, the neighborhood method "is a technique that classifies each record in a dataset based on the classes of the records" [1]. In short, the nearest neighborhood technique works by looking for similarities in data and making conclusions. Data that is similar to each other will have similar conclusions [2]. For example, if you look at people who live in the same area, it is safe to conclude the residents make a similar income [2].

The neighborhood technique seems very much alike the previously presented methods in that it groups data based off of attributes that the data possesses. It is essentially a refined version of clustering. Nevertheless, it is more advanced than clustering in that the algorithm weights importance and can detect which information is more influential in coming to a conclusion [2]. Not only that, another difference between clustering and neighborhoods is that clustering is an "unsupervised learning" technique, whereas neighborhoods is "supervised learning" [2]. Unsupervised learning sorts data without a purpose, while supervised learning categorizes it for the purpose of performing a prediction [2].

With neighborhoods as a way to mine data for the purpose of domestic security, it can be used to group data from various crimes and make a conclusion about these crimes, based upon finding the "nearest neighbor" or most similar attribute. A conclusion could be made to show the crimes were committed by the same perpetrators which would give detectives an advantage when trying to find who committed them [2].

2.2.2 Decision Trees

Decision trees are tree-shaped structures that map decisions which generate rules for the classification of a dataset [1]. In short, a decision tree is a predictive model [2]. The goal of a decision tree is to provide a set of rules that can be applied to unclassified data to predict a certain outcome [1]. The two most common types of data trees are Classification and Regression Trees (CART) and Chi Square Automatic Interaction Detection (CHAID).

CART trees is an algorithm structured as a series of questions where the answers determine the next question [2]. A good metaphor stated in Alex Berson's book on data mining, the CART method is essentially "growing a forest and picking the best tree" [2]. On the other hand, CHAID is a decision tree that weights significance of data and asks questions accordingly. Using CHAID is basically a different way to determine the questions that are asked. The major advantage of CHAID over CART is the simplicity of the results and its ability to handle large sample sizes [2].

2.2.3 Neural Networks

An artificial neural network, much like the biological neural network within the human brain, detect patterns, make predictions and learn. Networks estimate conclusions that are dependent upon a large number of inputs, some of which are unknown [2]. Neural networks are far more advanced than any of the previously discussed techniques. This method represents the cutting edge of data mining technology and its applications are endless. Neural networks can be used alone, or they can be used as a supplement to clusters, neighborhoods, classification, and decision trees to overall enhance the quality of the results [2].

A neural net is composed of two parts: the node and the link. The node is very much like a neuron in a human brain. The link is most closely associated with the connections between neurons (the axons, dendrites and synapses) in the human brain. It is important to understand that although neural networks stem from the Artificial Intelligence community, neural networks are not a form of artificial intelligence. Networks can only perform brain-like activity [2].

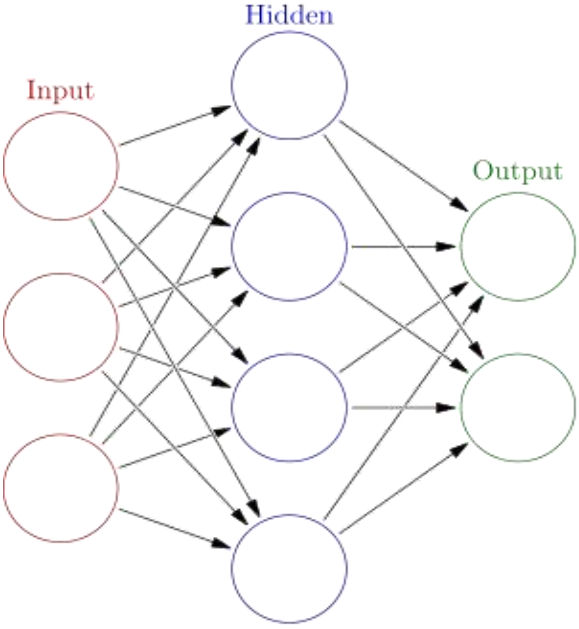


FIGURE 2 Above is a representation of a neural network; each circle is a node and each line is a link between the nodes and the outputs[2].

Although there are many different types of neural networks that have been created, the most used is the Kohonen feature maps. This algorithm is a simple version of neural networks, as it only has one input layer and one output layer. These levels compete amongst themselves to display the strongest conclusion [2]. Kohonen feature maps are extremely useful when combined with clustering. By making each output node a data cluster, each data byte would fall into only one cluster (the most common one). The other clusters that had less hits would still be shown, but they would be shown in the most likely to be the next best order. This is useful in that it allows the user to get a full analysis of all cluster categories [2].

In terms of security, neural networks are most commonly applied to clustering techniques. When networks are used for clustering, they are left in an unsupervised learning mode, or an autopilot-like setting where there is no user requesting specific types of conclusions. [2]. Therefore, the clusters the network creates are unbiased and may assist in finding patterns analysts would not have looked for otherwise. The clusters are formed by forcing the system to compress the data and create algorithms that create clusters that compete against one another for the information in the records it is sorting. This ensures the clusters overlap as little as possible, making the most useful and scientific analysis of the data [2].

2.2.4 Rule Induction

Rule induction is one of the most popular forms of data mining in terms of knowledge discovery. It is also the process that most closely resembles what a person thinks when he or she hears the word data mining because rule induction quite literally mines for information. A rule induction program mines for a rule that is interesting. This rule would point out a pattern in data that would be near impossible for a human to find [2].

In a rule induction program, all possible patterns are systematically pulled out of the data and then put through accuracy and significance tests. The accuracy test tells the user how 'true' the patterns predictions are. The significance test informs the user how widespread the pattern is. For example, if a pattern shows an outcome that is true 99% of the time, but it only applies to 20% of the data, this pattern is very accurate but low in significance. Since rule induction pulls so many patterns, the accuracy and significance test allows the program to rate which patterns may be of most use to the operator [2].

3. DATA MINING AND PRIVACY

In terms of privacy, data mining can be used to either protect it, or violate it. In order for data mining to be successful, the program needs to collect as much information as possible. To do this, many wish to cull mass amounts of information from computer users everywhere. This draws into question whether taking someone's online information is ethically plausible. It could also have a large effect on future generations and the durability of their future privacy rights. To attempt combat this ethical flaw, there is now research to see if there is a way to still have access to the information, without violating the privacy of the person whom the information came from.

3.1 Protecting Privacy

Often, data contained in a database is personal, therefore people want to protect it. A database that is mined may contain peoples' phone numbers, addresses and credit card information; however, a database could contain anything. Data-mining can be used to protect that information but, mining a database can also lead to a breach in the security of this personal information. However, that information, if used correctly, could be very beneficial.

The two most popular types of privacy-preserving data mining algorithms are k-anonymity and l-diversity. As a whole, privacy preservation involves using algorithms that either protect private data from the mining process itself or censor the results of the mine [5]. Both k-anonymity and l-diversity are of the former. They both use generalization and suppression methods to prevent the sensitive data from ever being mined in the first place and preserve the anonymity of the individuals to whom the data which is mined belongs to [5].

Algorithms, proposed by Stergios G. Tsiafoulis and Vasilis C. Zorkadis in their conference paper on preserving privacy in data mining, use clustering techniques to help ease the major concerns over the threat to privacy data mining poses. Their algorithm combines the concepts of k-anonymity, l-diversity and clustering to maximize the anonymity of the people whose data they are using. The goal of their algorithm is to be able to make use of the data, but not violate people's privacy [5].

First, the algorithm organizes data sets into subsets based off similarity; then it creates a more relevant group of classes based off of the attributes they are mining for, such as spending information. Finally, it attempts to generalize the information in order to preserve the privacy of the data's owner while preventing data loss [5]. However, the program's efficiency in preserving privacy can be questionable, as it is not perfect. For many, this program is not enough, as their private information is not generalized enough and may still be able to be linked to themselves, despite the attempt at anonymization. However, the program is meant to keep the "disclosure possibility" and "information loss" negligible, as stated by Stergios Tsiafoulis and Vasilis Zorkadis [5].

3.2 Data Mining and the Cloud

Today, the cloud is becoming an ever-increasingly popular method of storing data. It refers to servers accessed through the internet which store files and information that would normally be stored on local servers. With a constant increase in amounts of information being stored, many large companies are now using the cloud to store all of their private data. However, the cloud is considered to be very susceptible to hacking and malicious data mining [6]. Information companies tend to store information on the cloud including sales data, research and development data, and private information of the company's employees, such as their social security number. To help preserve the privacy of a company's data, Professors A. Bougettaya, X. Yi, F. Rao, and E. Bertino of the School of Computer Science and Information and Technology at RMIT University in Melbourne, Australia, propose an algorithm that uses decision trees to prevent hackers from mining their private data [6]. This is essentially using data mining techniques to prevent ill-purposed data mining.

This algorithm achieves that by first organizing that sensitive information into classes or clusters based on the importance of keeping that data private. The decision tree then places the data into separate servers with different levels of encryption depending on the level cluster or class [6]. Although the encryption can be broken through by advanced hackers, this greatly strengthens the security of the company from those who wish to do that company harm [6].

The algorithm could prove to be useful in protecting people's private information in a world that is increasingly moving towards cloud storage. This research also shows how data mining can be sustainable in terms of the continuation of personal privacy rights and demonstrates that data mining can be used to protect personal privacy as well as violate it.

4. DECISION TREES AND INTELLIGENCE

In today's age, intelligence wars are waged mostly on the computer in the form of intrusion, or the process of accessing a network without leaving a trace of a foreign presence [7]. To fight this, governments use different forms of Intrusion Detection Systems, or IDS's, to identify if an intrusion is threatening. IDS programs run through two detection programs, signature detection and anomaly detection.

Signature detection programs analyze known attacks to develop unique characteristics, or signatures, to compare to new intrusions in order to help identify if the attack is malicious or harmless [7]. However, this method does not work well with unknown attack methods. If an entirely new attack method is created, it may go undetected. Therefore, anomaly detection is a model built to describe normal behavior [6]. If any abnormal behavior is detected, it is flagged as a possible threat. However, this technique often leads to false alarms [7]. Even with the use of these two techniques, private networks can still be breached, although, by adding in a data mining tool, the defense algorithms can be more efficient and more expansive in identifying threats.

With the use of data mining, IDS's can quickly recognize data of interest to the user and efficiently sort it into categories based off of severity, complexity, or whatever else the user desires [7]. Figure 3 illustrates the decision process of an IDS integrated with data mining. Integrating data mining into the system allows the program to seize all of the information going to and from the network. This gives the user more information as to what is normal and what is an anomaly, allowing for the signature and anomaly techniques to be more inclusive in their data intake and more accurate in their conclusions [7].

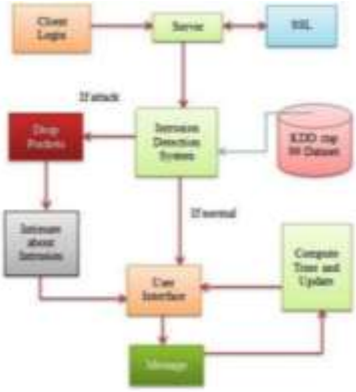


FIGURE 3 The above figure illustrates the decision process of a data mining integrated IDS[5].

M. Shree and J. Visumathi, professors of Computer Science and Engineering at Jeppiaar Engineering College in Chennai, India, proposed a Proficient Data Interested Decision Tree Algorithm (PDIDT) that integrates decision trees into signature and anomaly defense techniques [7]. The decision tree takes unique values and makes further decisions based off of previously defined classes [7]. It first takes a unique attribute of a possible intrusion and places that attribute into a class. It does this for as many attributes as the program can mine, then detects the probability of that combination of classes being threatening [7].

The incorporation of data mining and intelligence defense programs is a clear example of how data mining can be beneficial. This has the ability to protect people's rights to feel secure and improve the quality of life of the next generation. However, data mining used in this way also has the potential to violate the basic human right of privacy and, in turn, decrease the quality of life. Data mining assists governments in protecting sensitive information that, if revealed, could endanger lives of everyday citizens, soldiers and intelligence agents and assists in fighting the ever growing field of computer warfare.

5. CRIMINALS AND CLUSTERING

In modern criminal justice, all crimes are now documented on a computer. With this increased use of computerized systems, computer analysts have begun to assist law enforcement agencies to speed up the process of finding suspects and sorting relevant information for evidence [8]. S. Nath, a professor at Florida Atlantic University, has created a method that uses data mining, or, more specifically, clustering, to help identify patterns in crime [8].

The cluster method described by Professor Nath uses clustering to identify what type of crimes occur most commonly in a geographical location [8]. Nath prefers clustering over all other techniques because most criminal cases have missing information and clustering techniques are capable of predicting unknown information and can make connections a that human may not see [8]. These location based clusters are very useful in identifying a crime pattern or spree. This can be applied to serial killers, serial rapists or gang crimes due to the fact that these types of crimes often follow specific patterns [8].

Using the geographical based clusters, authorities are able to predict where a serial killer may strike next or where a gang's base is located. This is evidence of how data mining is beneficial and can help protect law-abiding citizens and prevent future crimes. However, due to security laws, information on many types of crimes, such as drugs and juvenile cases are more restricted as to who can access them [8]. This poses a problem for data analysts because clustering requires extensive information in order to make accurate conclusions. Since the data is limited, the conclusions have a larger margin for error, or may not have enough to make a proper conclusion. Also, analysts would need to be cautious with respect to where their data comes from and how it is mined in order to keep from breaking privacy laws. This once again brings up the issue of invading privacy with data mining. However, it could also be argued that incorporating data mining into crime investigation could help sustain a secure society in an increasingly dangerous world, improving the quality of life for future generations. Fortunately, data miners can work in accordance with the law to mine the proper crime data that is allowed for them to use.

6. COMPUTER ESPIONAGE

Today, one of the biggest threats to the United States is terrorism. Organizations like the National Security Agency, the Central Intelligence Agency and the Federal Bureau of Investigation are dedicated to preventing terrorist attacks and punishing the groups and individuals who commit them, from those deliberating within the country to those from foreign countries seeking to perform an act of terrorism. With the use of data mining, these government organizations are able to gather billions of pieces of data from phones, computers, Google, anything people use to communicate. With this data, operatives are able to make connections between people and help generate investigative leads [3]. To make these connections, analysts first tag all the data they have collected by sorting it into classes and clusters. From these classes and clusters, users analyze the data in an attempt to come to some conclusion about a possible attack, a possible suspect, or any potential threat to the country [3].

The tags that analysts collect operate by finding similarities and connections in video footage, audio tapes and phone records [3]. For example, data mining could flag a person who frequents terrorist websites or frequently search for words such as bomb-making and guns and put him or her on a watch list to help prevent a possible attack organized by this person [3].

The security advantages to data mining in this respect are evident. It helps the government prevent innocent citizens from violence and allows them to pursue criminals. However, when these organizations collect this data, they are not required to abide by the regular privacy laws and have access to information that usually requires a warrant [3]. No one monitors these organizations and how they are using this data. For many, this is a major breach in personal privacy and they believe it violates their constitutional rights. This is a major concern when it comes to the quality of life of future generations because they believe it is a violation of human rights. However, to others, the possible security benefits to the preservation of safety outweighs the potential violation of rights.

7. ETHICAL CONSEQUENCES OF DATA MINING

As useful as data mining is, many believe it is unethical and possibly dangerous for anyone to have access to all this information. Data mining can be used both to protect and to harm. It is a very powerful tool and some believe it could be abused. If data mining becomes widespread, it will have a large effect, both good and bad, on the quality of life of future generations. Debate can be stirred up as to how well it protects personal information. For instance, if a government uses data mining to find potential domestic terrorists through peoples' internet search history, that data is perhaps not being anonymized if it can be linked to the person that becomes a potential threat. Despite this, for many, the security benefits outweigh the security risks, so long as we keep data mining in the right hands.

7.1 Security Benefits

The security advantages of data mining are clear. The most obvious benefit however, is data mining's potential in protecting the average citizen. According to best-selling author and respected journalist, James Bamford, data mining could be "useful for everything from predicting humanitarian crises to directing rescue efforts during natural disasters [by making it] available to the world" [8]. When used correctly, data mining can help protect important intelligence by identifying cyber-attacks. If this intelligence went unprotected it could seriously endanger many lives. Decision trees vastly improve upon the efficiency of these defense algorithms. The use of clustering can also assist law enforcement to help solve and prevent crimes, lowering the crime rates and creating a safer living environment. One of the greatest advantages and most useful practices of data mining is for the government to apply it to homeland security. By using clustering and classes, government agencies are able to identify possible terroristic threats and track down the people who have already committed these acts, protecting citizens from possible harm.

Data mining also has the potential to greatly improve the lives of future generations. It can improve quality of life due to its potential to help protect people and preserve their ability to feel safe. With the use of data mining, governments can help prevent attacks, gain valuable intelligence, and preserve homeland safety. Data mining also benefits ordinary police departments as it could assist in catching dangerous criminals, profiling gang activity, and predict future crime. It is sustainable in that it can preserve the quality of life of the next generation.

Despite the worry that data mining invades people's privacy, there are data mining programs that preserve the anonymity of the people the data is from or mine around sensitive data. This eliminates some risk since, even if sensitive data comes to light, it would be difficult to link it to the individual that it came from.

7.2 Privacy Drawbacks

Despite the usefulness of data mining in terms of national security, it poses a large threat to personal security. In order to be efficient and accurate, data mining requires an expansive and all-encompassing data set. To get access to that amount of data, users collect data from everyone. This data could be phone records, personal videos and pictures, previous purchases, health records, and search histories. For many, this is a major invasion of privacy because, according to renowned author Elizabeth Svoboda, “some bit of seemingly harmless information that you post today could easily come back to haunt you years from now” [10]. The people who think data mining is unethical believe that the access to their personal information violates their constitutional rights and that any access to this information requires a warrant.

In terms of sustainability, many people believe that data mining is not sustainable because it will decrease the quality of life of future generations. This point of view is based on the belief that data mining violates human rights because it violates people’s basic desire for privacy. This violation of rights cancels out any benefits data mining might have. Many believe that the breach of human rights outweighs any positive effects on the quality of life that more advanced security could have. Opponents to data mining conclude that although data mining can improve domestic security, it breaches personal security along the way [10].

8. THE RESULTS: DO THE BENEFITS OUTWEIGHT THE RISKS?

After careful consideration of all the potential benefits and potential pitfalls of data mining, we can conclude that data mining is a useful tool which should be used by the government to enhance security. The main concern that is cited when people argue against data mining is the invasion of privacy through the gathering of everybody’s personal data. However, steps can be taken to anonymize the data so it cannot be connected to the individuals that it came from unless those individuals pose a threat. Collection of this data may be considered an invasion of privacy, but this is irrelevant if the data cannot be connected to the person. Mining anonymized data cannot be a violation of privacy, since the data has no face behind it.

Data mining can also be seen as a benefit from the sustainability point of view. It can greatly improves the quality of life for future citizens. The belief that data mining decreases quality of life by violating privacy rights is outweighed by the security benefits it provides. As social media and internet use becomes more popular, the value of privacy drops. Already the younger generations post all of their private information on the internet through social media. The value of privacy is decreasing; however, the value of personal safety will never decrease. From catching criminals to protecting sensitive intelligence, the uses and advantages of data mining are worth the risk.

9. REFERENCES

[1] J. Frand. (2010). “Data Mining: What is Data Mining?”. (online article). http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm

[2] A. Berson. (2012). “Building Data Mining Applications for CRM (Enterprise)”. McGraw-Hill Education. (Print book).

[3] J. Pappalardo. (2013, Oct.). “NSA Data Mining: How It Works.” Popular Mechanics. (online article). DOI: 00324558

[4] M. Brown. (2014). “Data mining techniques.” developerWorks. (online article). http://www.ibm.com/developerworks/library/ba-data-mining-techniques/ba-data-mining-techniques-pdf.pdf

[5] G. Tsiafoulis, C. Zorkadis. (2012). “A neural-network clustering-based algorithm for privacy preserving data mining.” Computational Intelligence and Security (CIS). (online article). ISBN: 978-1-4244-9114-8. pp. 401-405

[6] A. Bouguettaya, X. Yi, F. Rao, E. Bertino (2015). “Privacy-Preserving Association Rule Mining in Cloud Computing.” 10th ACM Symposium on Information, Computer and Communications Security. (online article). ISBN: 978-1-4503-3245-3.

[7] M. Shree, J. Visumathi, P. Jayarin. (2016). “Identification of attacks using proficient data interested decision tree algorithm in data mining.” Advances in Intelligent Systems and Computing. (online article). DOI: 10.1007/978-81-322-2674-1_60

[8] S. Nath. (2016, Dec.). “Crime Pattern Detection Using Data Mining.” Web Intelligence and Intelligent Agent Technology. (online article). DOI: 10.1109/WI-IATW.2006.55

[9] J. Bamford. (2015). “The Black-and-White Security Question.” Foreign Policy. (print article). pp.70-75

[10] E. Svoboda. (2009). “Digital Exposure.” Discover. (print article). Vol. 30, Issue 10

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 478 – 483, 2016, ISSN: - 2319-8656

An proficient and Confidentiality-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

Dr V. Goutham
Teegala Krishna Reddy
Engineering College
Meerpet,Telangana,India

B.Shyla Reddy
Teegala Krishna Reddy
Engineering College
Meerpet, Telangana,India

.Krishna Manasa
Teegala Krishna Reddy
Engineering College
Meerpet, Telangana,India

Abstract: Cloud computing has developed progressively prevalent for data owners to outsource their data to public cloud servers while consenting data users to reclaim this data. For isolation disquiets, a secure rifle over encrypted cloud data has stirred numerous research mechanisms underneath the particular owner model. Conversely, most cloud servers in practice do not just assist one owner, as an alternative, their sustenance gives multiple owners to share the assistances carried by cloud computing. In this proficient and confidentiality-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, new schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM) has been introduced. To facilitate cloud servers to execute secure search without knowing the actual data of both keywords and trapdoors, we thoroughly build a novel secure search protocol. To rank the search results and domain the privacy of relevance scores amongst keywords and files. To thwart the assailants from snooping secret keys and fantasizing to be legal data users submitting pursuits, a novel dynamic secret key generation protocol and a new data user authentication protocol is discussed.

Keywords: Cloud computing, ranked keyword search, multiple owners, privacy preserving, dynamic secret key

1. INTRODUCTION

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements regardless of where the services are hosted. Several computing paradigms have promised to deliver this utility computing vision. Cloud computing is the most recent emerging paradigm promising to turn the vision of "computing utilities" into reality. A service offering computation resources is frequently referred to as Infrastructure as a Service (IaaS) and the applications as Software as a Service (SaaS)[1]. An environment used for construction, deployment, and management of applications is called PaaS (Platform as a Service).

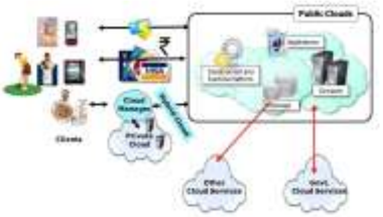


Fig.1: A bird's eye view of Cloud computing

Cloud computing delivers infrastructure, platform, and software (application) as services, which are made available as subscription-oriented services in a pay-as-you-go model to consumers. The price that CSPs (Cloud Service Providers) charge depends on the quality of service (QoS) expectations of CSCs (Cloud Service Consumers).Cloud computing fosters elasticity and seamless scalability of IT resources that are offered to end users as a service through the Internet. Cloud computing can help enterprises improve the creation and delivery of IT solutions by providing them with access to services in a cost-effective and flexible manner [2]. Clouds can be classified into three categories, depending on their accessibility restrictions and the deployment model. They are:

- Public Cloud,
- Private Cloud, and
- Hybrid Cloud.

A public Cloud is made available in a pay-as-you-go manner to the general public users irrespective of their origin or affiliation. A private Cloud's usage is restricted to members, employees, and trusted partners of the organization. A hybrid Cloud enables the use of private and public Cloud in a seamless manner. Cloud computing applications span many domains, including business, technology, government, health care, smart grids, intelligent transportation networks, life sciences, disaster management, automation, data analytics, and consumer and social networks. Various models for the creation, deployment, and delivery of these applications as Cloud services have emerged.

Cloud service providers (CSPs) would promise to certify owners' data security using purposes like virtualization and firewalls. Conversely, these mechanisms do not protect owners' data privacy from the CSP itself, since the CSP holds full control of cloud hardware, software, and owners' data. Encryption on sensitive data formerly subcontracting can realm data privacy beside CSP. Nevertheless, data encryption sorts the traditional data utilization service based on plaintext keyword search a very perplexing delinquent. A trifling solution to this problem is to move all the encrypted data and decrypt them nearby. Nonetheless, this method is evidently impracticable since it will cause a huge amount of communication overhead. Consequently, emerging a secure search service over encrypted cloud data is of overriding prominence. Secure search over encrypted data has recently attracted the interest of many researchers. Song et al. [3] first define and solve the problem of secure search over encrypted data. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset. Searchable encryption is additionally developed by [4], [6]. However, these schemes are concerned mostly with single or boolean keyword search. Encompassing these procedures for ranked multikeyword search will acquire heavy computation and storage costs. The main contributions of this proficient and confidentiality-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data are listed as Follows: (a) a multi-owner model for privacy preserving keyword search over encrypted cloud data is defined. (b) an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation is defined. (c) a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys is systematically constructed.

2. RELATED WORK

2.1 Searchable Encryption

The earliest attempt of searchable encryption was made by Song et al. In [3], they propose to encrypt each word in a file independently and allow the server to find whether a single queried keyword is contained in the file without knowing the exact word. This proposal is more of theoretic interests because of high computational costs. Goh et al. propose building a keyword index for each file and using Bloom filter to accelerate the search [4]. Curtmola et al. propose building indices for each keyword, and use hash tables as an alternative approach to searchable encryption [5]. The first public key scheme for keyword search over encrypted data is presented in [6]. [7] and [8] further enrich the search functionalities of searchable encryption by proposing schemes for conjunctive keyword search. The searchable encryption cares mostly about single keyword search or boolean keyword search. Extending these techniques for ranked multi-keyword search will incur heavy computation and storage costs.

2.2 Secure Keyword Search in Cloud Computing

The privacy concerns in cloud computing motivate the study on secure keyword search. Wang et al. first defined and solved the secure ranked keyword search over encrypted cloud data. In [9] and [18], they proposed a scheme that returns the top-*k* relevant files upon a single keyword search. Cao et al. [10], [11], and Sun et al. [1], [12] extended the secure keyword search for multi-keyword queries. Their approaches vectorize the list of keywords and apply matrix multiplications to hide the actual keyword information from the cloud server, while still allowing the server to find out the top-*k* relevant data files. Xu et al. proposed MKQE (Multi-Keyword ranked Query on Encrypted data) that enables a dynamic keyword dictionary and avoids the ranking order being distorted by several high frequency keywords [13]. Li et al. [4], Chuah et al. [15], Xu et al. [16] and Wang et al. [7] proposed fuzzy keyword search over encrypted cloud data aiming at tolerance of both minor misprints and format inconsistencies for users' search input. [19] further proposed privacy-assured similarity search mechanisms over outsourced cloud data. In [10], a secure, efficient, and distributed keyword search protocol in the geo-distributed cloud environment. The system model of these previous works only consider one data owner, which implies that in their solutions, the data owner and data users can easily communicate and exchange secret information. When numerous data owners are involved in the system, secret information exchanging will cause considerable communication overhead. Sun et al. [2] and Zheng et al. [12] proposed secure attribute-based keyword search schemes in the challenging scenario where multiple owners are involved. However, applying CPABE in the cloud system would introduce problems for data user revocation, i.e., the cloud has to update the large amount of data stored on it for a data user revocation [14]. Additionally, they do not support privacy preserving ranked multi-keyword search. An proficient and confidentiality-Preserving Multi-

Keyword Ranked Search over Encrypted Cloud Data differs from previous studies regarding the emphasis of multiple data owners in the system model. An proficient and confidentiality-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data seeks a solution scheme to maximally relax the requirements for data owners and users, so that the scheme could be suitable for a large number of cloud computing users.

2.3 Order Preserving Encryption

The order preserving encryption is used to prevent the cloud server from knowing the exact relevance scores of keywords to a data file. The early work of Agrawal et al. proposed an Order Preserving symmetric Encryption (OPE) scheme where the numerical order of plain texts are preserved [13]. Boldyreva et al. further introduced a modular order preserving encryption in [4]. Yi et al [5] proposed an order preserving function to encode data in sensor networks. Popa et al. [6] recently proposed an ideal-secure order-preserving encryption scheme. Kerschbaum et al. [7] further proposed a scheme which is not only idea-secure but is also an efficient order-preserving encryption scheme. However, these schemes are not additive order preserving. As a complementary work to the previous order preserving work, a new additive order and privacy preserving functions (AOPPF) are proposed. Data owners can freely choose any function from an AOPPF family to encode their relevance scores. The cloud server computes the sum of encoded relevance scores and ranks them based on the sum.

3. SYSTEM DESIGN

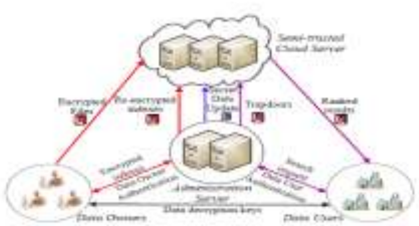


Fig. 1: Architecture of privacy preserving keyword search in a multi-owner and multi-user cloud model

3.1 Design Goals:

3.1.1 Ranked Multi-keyword Search over Multi owner:

The projected system should consent multi-keyword search over encrypted files which would be encrypted with dissimilar keys for altered data owners [10]. It also needs to allow the cloud server to rank the search results among unlike data owners and return the top-*k* results.

- **Data owner scalability:** The projected system should allow new data owners to enter this system without disturbing other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model.
- **Data user revocation:** The projected system should ensure that only legitimate data users can perform correct rifles [9]. Moreover, once a data user is revoked, he can no longer perform accurate searches over the encrypted cloud data.
- **Security Goals:** The projected system should achieve the following security goals: 1) Keyword Semantic Security (Definition 1). We will prove that PRMSM achieves semantic security against the chosen keyword attack. 2) Keyword secrecy (Definition 2). Since the adversary *A* can know whether an encrypted keyword matches a trapdoor, we use the weaker security goal (i.e., secrecy), that is, we should ensure that the possibility for the adversary *A* to conclude the actual value of a keyword is insignificantly more than arbitrarily predicting [12]. 3) Relevance score secrecy. We should ensure that the cloud server cannot conclude the actual value of the encoded relevance scores.

3.2 Data User Authentication

To thwart attackers from pretending to be legal data users accomplishing searches and hurling statistical attacks based on the search result, data users must be authenticated before the administration server re-encrypts trapdoors for data users. Conventional authentication methods often follow [18] three steps. First, data requester and data authenticator share a secret key. Second, the requester encrypts his individually recognizable information and sends the encrypted data to the authenticator. Third, the authenticator decrypts the received data with and authenticates the decrypted data. Conversely, this method has two main drawbacks [17]. Since the secret key shared between the requester and the authenticator remains unaffected, it is easy to acquire repeat attack. Second, once the secret key is discovered to attackers, the authenticator cannot discriminate between the legal requester and the attackers[16]; the attackers can made-up to be legal requesters without being detected.

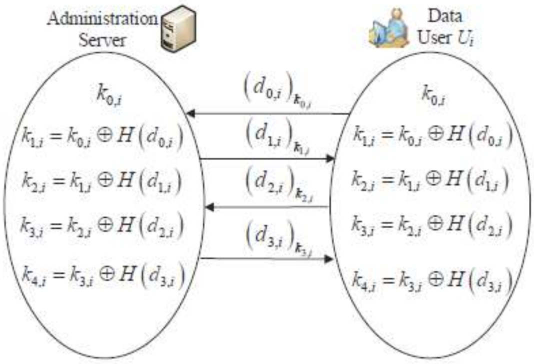

Administration Server
Data User U_i
$k_{0,i}$
$k_{1,i} = k_{0,i} \oplus H(d_{0,i})$
$k_{2,i} = k_{1,i} \oplus H(d_{1,i})$
$k_{3,i} = k_{2,i} \oplus H(d_{2,i})$
$k_{4,i} = k_{3,i} \oplus H(d_{3,i})$
$(d_{0,i})_{k_{0,i}}$
$(d_{1,i})_{k_{1,i}}$
$(d_{2,i})_{k_{2,i}}$
$(d_{3,i})_{k_{3,i}}$
$k_{0,i}$
$k_{1,i} = k_{0,i} \oplus H(d_{0,i})$
$k_{2,i} = k_{1,i} \oplus H(d_{1,i})$
$k_{3,i} = k_{2,i} \oplus H(d_{2,i})$
$k_{4,i} = k_{3,i} \oplus H(d_{3,i})$

Fig.2: Example of data user authentication and dynamic Secret key generation

3.3 Data User Revocation

Dissimilar from previous works, data user revocation in this scheme does not need to re-encrypt and update large amounts of data stored on the cloud server. The administration server only needs to update the secret data stored on the cloud server. Accordingly, the earlier trapdoors will be perished [14]. Furthermore, without the help of the administration server, the repealed data user cannot produce the correct trapdoor. Hence, a data user cannot perform correct searches once he is revoked.

3.4 Keyword Encryption

For keyword encryption, the following conditions should be satisfied: first, distinct data owners use their own secret keys to encrypt keywords. Second, for the same keyword, it would be encrypted to distinct cipher-texts each time[15]. These belongings benefit the scheme for two reasons. First, losing the key of one data owner would not lead to the revelation of other owners' data[13]. Second, the cloud server cannot see any relationship among encrypted keywords.

3.5 Trapdoor Generation

To make the data users produce trapdoors securely, conveniently and efficiently, our projected system should mollify two main conditions. First, the data user does not need to ask a large amount of data owners for secret keys to engender trapdoors. Second, for the same keyword, the trapdoor generated each time should be distinct [12]. To meet this condition, the trapdoor generation is conducted in two steps: First, the data user produces trapdoors based on his search keyword and a random number. Second, the administration server re-encrypts the trapdoors for the authenticated data user [19].

3.6 Keywords Matching among Distinct Data Owners

The cloud server stores all encrypted files and keywords of distinct data owners. The administration server will also store a secret data on the cloud server. Upon receiving a query request, the cloud will examine over the data of all these data owners[17]. The cloud processes the search request in two steps. First, the cloud contests the queried keywords from all keywords stored on it, and it gets a candidate file set. Second, the cloud ranks files in the candidate file set and finds the most top-*k* relevant files [18].

4. PROJECTED SYSTEM : PRIVACY PRESERVING RANKED SEARCH

The aforesaid section helps the cloud match the queried keywords, and acquire a candidate file set. Nonetheless, we cannot simply return non-distinct files to data users for the following two reasons. First, returning all candidate files would cause abundant communication overhead for the whole system. Second, data users would only apprehend the top-*k* relevant files corresponding to their queries [16]. We initially elucidate an order and privacy preserving encoding scheme. An additive order preserving and privacy preserving encoding scheme is demonstrated. The projected system to encode the [20] relevance scores and obtain the top-*k* search results is conferred.

4.1 Order and Privacy Preserving Function:

To rank the consequence score while preserving its privacy, the proposed function should satisfy the following conditions. 1) This function should preserve the order of data, as this helps the cloud server determine which file is more relevant to a certain keyword, according to the encoded relevance scores. 2) This function should not be revealed by the cloud server so that cloud server can make associations on encoded relevance scores without knowing their actual values. 3) Distinct data owners should have distinct functions such that enlightening the encoded value of a data owner would not lead to the leakage of encoded values of other data owners[19].

4.2 Ranking search results

In proficient and confidentiality-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, the sum of the relevance scores as the metric to rank search results is used. The strategies of ranking search results based on the encoded relevance scores is introduced. First, the cloud computes the sum of encoded relevance scores between the file and matched keywords. Then the cloud ranks the sum of encoded relevance score with the following two conditions: (1) Two encoded data belong to the same data owner. Given that a data user issues a query and satisfies the[16] query. Then the cloud adds the encoded relevance score together and gets the relevance score.

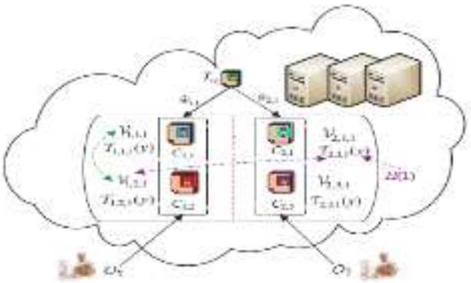
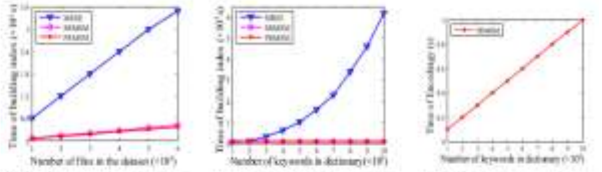


Fig. 3: Example of ranking search results

5. EXPERIMENTAL EVALUATION

The efficiency of PRMSM is measured and compared it with its previous version, Secure Ranked Multi-keyword Search for Multiple data owners in cloud computing (SRMSM) [17], and the state of- the-art, privacy-preserving Multi-keyword Ranked Search over Encrypted cloud data (MRSE) [11], side by side. Since MRSE is only suitable for the single owner model, our PRMSM and SRMSM not only work well in multi-owner settings, but also outpace MRSE on many aspects.

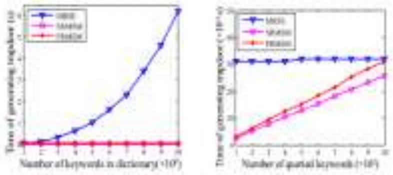


(a) For different size datasets with the same dictionary, u = 4000.

(b) For the same dataset with different dictionary sizes, n = 1000.

(c) Time cost of encoding relevance score (a subroutine of building index)

Fig. 6: Time cost of index construction.



(a) For different size of keyword dictionary with the same number of queried keywords, q = 100.

(b) For different number of queried keywords with the same size of keyword dictionary, u = 4000.

The experiment programs are coded using the Python programming language on a PC with 2.2GHZ Intel Core CPU and 2GB memory. We implement all necessary routines for data owners to preprocess data files: [13],[10]for the data user to generate trapdoors, for the administrative server to re-encrypt keywords, trapdoors, and for the cloud server to perform ranked searches.

5.1 Index Construction

Fig. 6(a) shows that, given the same keyword dictionary (u=4000), time of index construction for these schemes escalate linearly with an increasing number of files, while SRMSM and PRMSM spend much less time on index construction. Fig. 6(b) reveals that, given the same number of files (n=1000), SRMSM and PRMSM ingest much less time than MRSE on constructing indexes. Furthermore, SRMSM and PRMSM are insensitive to the size of the keyword dictionary [9],[20]for index construction, while MRSE suffers a quadratic growth with the size of keyword dictionary increases. Fig. 6(c) shows the encoding efficiency of our proposed AOPPF. The time spent on encoding increases from 0.1s to 1s when the number of keywords increases from 1000 to 10000. This time cost can be suitable.

5.2 Trapdoor Generation

Linked with index construction, trapdoor generation consumes relatively less time. Fig. 7(a) demonstrates that, given the same number of queried keywords (q=100), SRMSM and PRMSM are insensitive to the size of keyword dictionary on trapdoor generation and guzzles 0.026s and 0.031s, correspondingly. Temporarily, MRSE increases from 0.04s to 6.2s. Fig. 7(b) shows that, given the same number of dictionary size (u=4000), [17]when the number of queried keywords increases from 100 to 1000, the trapdoor generation time for MRSE is 0.31s, and remains unchanged. While SRMSM increases from 0.024s to 0.25s, PRMSM increases from 0.031s to 0.31s. We notice that PRMSM spends a little more time than SRMSM on trapdoor generation; the reason is that PRMSM familiarizes a further variable to ensure the randomness of trapdoors.

6. CONCLUSION

In proficient and confidentiality-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, the tricky of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Distinct from prior works, these schemes enable authenticated data users to achieve secure, expedient, and effectual searches over several data owners' data. To proficiently substantiate data users and distinguish attackers who steal the secret key and execute illegal searches, a novel dynamic secret key generation protocol and a innovative data user authentication protocol is discussed. To support the cloud server to accomplish secure search amid multiple owners' data encrypted with distinct secret keys, we thoroughly construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Besides, it is shown that the slant is computationally effective, even for large data and keyword sets. The future work will consider the delinquent of secure fuzzy keyword search in a multi-owner paradigm and to implement the present scheme on the viable clouds.

7. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Communication of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE International Symposium on Security and Privacy (S&P'00)*, Nagoya, Japan, Jan.2000, pp. 44–55.

[4] E. Goh. (2003) Secure indexes. [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. ACM CCS'06*, VA, USA, Oct. 2006, pp. 79–88.

[6] D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *EUROCRYPT*, vol. 43, pp. 506–522, 2004.

[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Proc. Applied Cryptography and Network Security (ACNS'04)*, Yellow Mountain, China, Jun. 2004, pp. 31–45.

[8] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in *Proc. Information and Communications Security (ICICS'05)*, Beijing, China, Dec. 2005, pp. 414–426.

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. IEEE Distributed Computing Systems (ICDCS'10)*, Genoa, Italy, Jun. 2010, pp. 253–262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data," in *Proc. IEEE INFOCOM'11*, Shanghai, China, Apr. 2011, pp. 829–837.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," *Parallel and Distributed Systems, IEEE Transactions on*,vol. 25, no. 1, pp. 222–233, 2014.

[12] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 11, pp. 3025–3035, 2014.

[13] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multikeyword ranked query on encrypted data in the cloud," in *Proc. IEEE Parallel and Distributed Systems (ICPADS'12)*, Singapore, Dec. 2012, pp. 244–251.

[14] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. IEEE INFOCOM'10*, San Diego, CA, Mar. 2010, pp. 1–5.

[15] M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in *Proc. IEEE 31th International Conference on Distributed Computing Systems (ICDCS'11)*, Minneapolis, MN, Jun. 2011, pp. 383–392.

[16] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *Computers, IEEE Transactions on*, vol. 62, no. 11, pp. 2266–2277, 2013.

[17] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in *IEEE INFOCOM*, Toronto, Canada, May 2014, pp. 2112–2120.

[18] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 8, pp. 1467–1479, 2012.

AUTHORS

[1] Dr V. Goutham is a Professor and Head of the Department of Computer Science and Engineering at TEEGALA KRISHNA REDDY ENGINEERING COLLEGE affiliated to J.N.T.U Hyderabad. He received Ph.d from Acharya Nagarjuna University and M.Tech from Andhra University. He worked for various MNC Companies in Software Testing and Quality as Senior Test Engineer. His research interests are Software Reliability Engineering, software testing, software Metrics, and cloud computing.

[2] Mr.B.Shyla Reddy is working as an Assistant Professor in the Department of Computer Science and Engineering at TEEGALA KRISHNA REDDY ENGINEERING COLLEGE affiliated to J.N.T.U Hyderabad. He received M.Tech from JNTU Hyderabad. His research interests are Database, Networking and Cloud computing.

[3] Ch.Krishna Manasa Department of Computer Science and Engineering at TEEGALA KRISHNA REDDY ENGINEERING COLLEGE affiliated to J.N.T.U Hyderabad.

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 484 – 488, 2016, ISSN: - 2319-8656

Intel Microprocessors- a Top down Approach

Muhammad Irfan[1], Jan Sher[1], Naveed Ullah[1], Muhammad Sulaiman[1], Junaid Saleem[1,]
[1]Department of computer science, Abdul Wali Khan University Mardan, KPK, Pakistan

Abstract- IBM is the world's largest manufacturer of computer chips. Although it has been challenged in recent years by newcomers AMD and Cyrix, Intel still Predominate the market for PC microprocessors. Nearly all PCs are based on Intel's x86 architecture. IBM (International Business Machines)IBM (International Business Machines) is by far the world's largest information technology company in terms of Gross ($88 billion in 2000) and by most other measures, a position it has held for about the past 50 years. IBM products include hardware and software for a line of business servers, storage products, custom-designed microchips, and application software. Increasingly, IBM derives revenue from a range of consulting and outsourcing services. In this paper we will compare different technologies of computer system, its processor and chips.

Keywords: Intel, Microprocessor, Server, PCs

I. INTRODUCTION

Intel is the American company headquartered in Santa Clara, California. Intel is one of the world largest and highest valued semiconductor chip makers, based on Gross. It is the Discoverer of the x86 series of microprocessors, the processors found in most personal computers. Intel supplies processors for computer system manufacturers such as Apple, Samsung, HP and Dell. Intel also makes motherboard chipsets, network interface controllers and integrated [1, 2] circuits, flash memory, graphics chips, embedded processors and other devices related to communications and computing. Intel Corporation was founded on July 1968 by semiconductor Innovators Robert Noyce and Gordon Moore and to a great degree associated with the executive (Administrator) leadership and Imagination of Andrew Grove, Intel combines advanced chip design capability with a leading-edge manufacturing capability. Intel was an early developer of SRAM and DRAM memory chips [3-8], which represented the majority of its business until 1981. Although Intel created the world's first commercial microprocessor chip in 1971, it was not until the success of the personal computer (PC) that this became its primary business. During the 1990s, Intel invested heavily in new microprocessor designs fostering the rapid growth of the computer industry During this period Intel became the dominant supplier of microprocessors for PCs, and was known for aggressive and anti-competitive tactics in defense of its market position, particularly against Advanced Micro Devices (AMD), as well as a struggle with Microsoft for control over the direction of the PC industry.

II. HARDWARE SPECIFICATIONS

We'll compare Intel's Xeon E5-2698 v3 (Haswell) and IBM's ISeries 8286-42A (POWER8) processors for our test applications. The test application is a Monte-Carlo simulation, pricing a portfolio of LIBOR swaptions [9-14] and simultaneously computing first order sensitivities (Greeks) to the initial forward rates using path-wise Adjoint Algorithmic Differentiation (AD). The LIBOR market model is applied to simulate thousands of possible future development paths for the LIBOR forward rates, using normally-distributed random numbers. Within each of these Monte-Carlo paths, the value of the swaption portfolio [15] is then calculated by applying a portfolio payoff function. For ad joint differentiation, the algorithm is then executed in reverse to find the Greeks. To obtain the final results, both the price and the Greeks are averaged across all paths [16, 17].

The processing graph in Figure 1 illustrates the application:

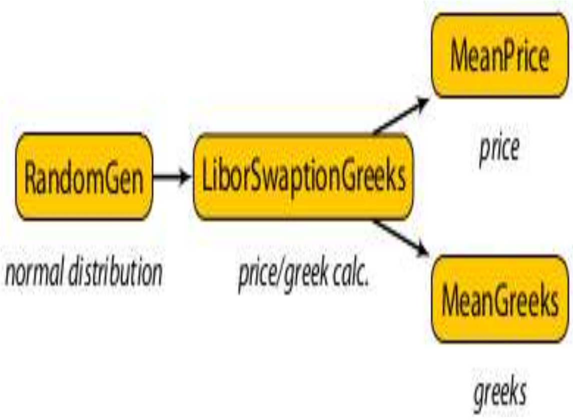


Figure 1: Processing Graph

III. BENCHMARK SETUP

The test systems had the following configuration:

- **CPU:** 2x Intel Xeon E5-2698 v3 (HT on) and 2 x POWER8 8286-42A (SMT on)
- **OS:** RedHat Enterprise Linux 6.6 and Ubuntu 14.10
- **RAM:** 256GB
- **Compiler:** Intel Compiler 15.0 and IBM Compiler 13.1

The application was compiled with maximum optimization settings, fast math mode, and tuning for the target processor architecture. The generated code makes extensive use of low-level processor features, such as vector extensions, fused [17-22] multiply-add instructions, cache optimizations, etc.

IV. INTEL vs. IBM

POWER8-based uniprocessor/dual processor systems can execute more work more quickly than Intel E5 7v2 Xeon-based servers. POWER8 can process four times as many threads as its E5 v2 competitors; the POWER8 clock speed is faster; and POWER8 can work on significantly more data in cache than E5 v2-based servers. Furthermore, POWER8 memory bandwidth is much faster than the Intel environment. What all of this means is that POWER8-based servers can outperform E5 v2-based servers (helping enterprises achieve results more quickly); and POWER8-based servers are also more efficient (meaning that enterprises will not need to buy as many servers to execute workloads. This will help enterprises save BIG MONEY by not having to purchase as many software licenses).

1. Both microprocessor/server environments have been designed to process Web, file and print, email, database, vertical-specific applications, high performance computing and cloud workloads;
2. POWER8 processors are more efficient than Xeon processors;
3. Due to processing and bandwidth advantages, POWER8-based servers can deliver results more quickly.
4. POWER8-based servers are better suited for data-intensive environments; and,
5. When executing identical workloads, POWER8-based servers will cost less that E5 v2-based competitors (due to aggressive IBM pricing and numerous efficiency advantages).

V. BACKGROUND

In June, 2013, Intel released the first member of its dual processor E5 v2 family – the Xeon E5-2692 v2 (Intel now offers 38 different E5 v2 processors that operate at varying speeds, with from four to fifteen cores per processor). These processors have been designed largely to serve the Windows and Linux marketplaces [23-28]. There is a lot to like about this family of microprocessors as compared with the previous Xeon generation because these processors (codenamed “Ivy Bridge”) offer more cores, more cache, faster speed, lower energy consumption, and reliability/avail-ability/serviceability extensions). But probably the biggest improvement in Xeon v2 architecture is the amount of main memory that can now be addressed [29-33]. With v2 architecture, x86 servers will

Someday be able to address up to 16TB of main memory in large, scale-up configurations. Clabby Analytics is impressed with both architectures. We like the way Intel has finally addressed the memory limitations of scale-up x86 architectures (the subject of this report). But we are especially impressed with the processor efficiency, performance and bandwidth improvements offered with POWER8-based systems. With a faster clock speed; with the ability to process four times as many threads per cycle as x86 processors; with three times more on-chip cache; with four to six times the memory bandwidth – and with access to up to 80 TB of Flash using the newly introduced coherence attached processor interface (CAPI) – IBM has created a systems environment with POWER8 that has been designed to very significantly outperform Intel Xeon architecture. The way we see it, this new generation of POWER8-based servers has literally been “designed for data”. We see the current generation of single and dual-socket systems as a true threat to the x86 dominance of the scale-out Linux marketplace. And, as larger and large configurations come to market, we expect to see a lot of POWER8-based servers configured for large database-in-memory processing – and given POWER8 performance advantages, these new in-memory servers will raise the performance bar for database processing in the future. The Primary Differentiators: Performance and Efficiency As we compared Intel’s Xeon E5-2692 v2 with IBM’s POWER8 architecture from both a processor design and subsystem perspective [34], it became readily apparent that both chips were designed to process serial, parallel and data-intensive workloads – but it also became clear that IBM’s POWER8 architecture was designed to deliver high-performance while operating far more efficiently [35] than Intel’s Xeon architecture.

To illustrate these points, consider the following: Performance – IBM’s POWER8 is more than 25% faster per clock cycle than Intel’s E5-2692 v2 (IBM operates at 4.15 GHz per clock cycle; Intel’s E5-2692 v2 runs at 2.697 GHz). POWER8 offers three times more on-chip cache (data in cache can be read faster – leading to faster performance and faster results). Further, POWER8 can address almost 25% more main memory than the E5-2692 v2 – again placing more data closer to the processor where it can be read and acted-on more quickly. And POWER8 can receive data from memory four to six times faster than Xeon bus can. The combination of a faster processor with access to more cache and memory – with significantly faster memory bandwidth – make POWER8 processors more powerful than Xeon E5 architectures. Efficiency – POWER8 offers a 12 core processor configuration that can process 8 threads per core (or 96 threads simultaneously per clock cycle). By comparison, Intel's E5-2697) has 12 cores but can only process two threads per core for a total of only 24 threads per clock cycle. This one design difference – processor efficiency – is extremely important when comparing POWER architecture to Xeon x86 architecture. A single 12 core POWER8 processor can process over three times as much data per clock cycle as compared to a 12 core Xeon E5-2697. What this means is that it could take up to three Xeon servers to do the work of a single POWER8-based server. It also means x86 buyers would potentially need to purchase up to three times the number of software licenses when opting for a Xeon-based server solution. Figure 2 presents a side-by-side comparison of Intel's Xeon E5-2697 v2 versus IBM's POWER8architecture. Especially important to note are: 2. The # of threads/core (POWER8 can process 8 threads per core per clock cycle to Intel's two threads) – this gives IBM a huge processor efficiency advantage over Xeon;

The amount of data that can be placed in cache (POWER8 offers over three times as much cache). It should also be noted that POWER8 can also make use of 128 MB eDRAM L4 cache that resides just off the chip. All of this close-proximity cache gives IBM's POWER8 a huge data processing speed advantage over Intel's Xeon E5 architecture; and, 3. The memory bandwidth speed (POWER8 is almost four times faster than Xeon).

In addition to huge performance and efficiency advantages, IBM has also "CAPI-enabled" its POWER8 processors. With POWER8, IBM has placed PCIe Gen 3 logic directly on the chip – andhas built an interface to this logic known as the coherence attached processor interface (or CAPI). As illustrated in Figure 2, CAPI is a customizable hardware accelerator that enables devices, Flash and coprocessors to talk directly and at very high speeds with POWER8 processors. Xeon offers a similar interface known as Quick Path Interconnect (QPI) – the primary differentiator [36] is that CAPI is an open interface while QPI is not.

VI. SUMMARY OBSERVATIONS

When selecting computer systems, the primary goal of information technology (IT) decision makers should be to pick the computer system best suited to most efficiently execute assigned workloads. By choosing the right information systems IT executives can lower computing costs (because fewer computing systems are needed, and because fewer software licenses will be required). Further, more efficient systems often yield faster computing results (a Quality-of-Service [QoS] consideration). Accordingly, the choice of infrastructure (microprocessors, system designs, systems software) matters tremendously. The major differentiators when comparing Xeon 35 v2 processors with POWER8 microprocessors can be found in performance and efficiency:

1. Performance – POWER8's clock speed is almost 25% faster than the E5-2692; it has access to three times more on-chip cache – and data in memory can be fed to POWER8 which is four times faster than its Xeon competitor. This kind of optimization makes POWER8 a Formidable competitor – especially when running data-intensive applications.
2. Efficiency – When running the same workload on a POWER8 as compared with a Xeon E5 Competitor, expect more work to be processed per clock cycle (to be precise, expect three Infrastructure Matters: POWER 8-based Power Systems vs. x86 Servers
3. Times as much work to be processed per clock cycle). Because POWER8 can process more work More quickly, expect to have to use fewer POWER8-based systems to handle an identical workload (Or expressed differently, expect to need to purchase up to three Xeon E5-based servers to handle

4. The same amount of work as a POWER8-based server. Also expect to spend up-to three times more money for additional software licenses). IBM's POWER8 announcement focused quite a bit on the performance and efficiency benefits that Can be derived by adopting POWER8-based scale-out Power Systems. But we are also intrigued by some of the new innovations taking place within the Power Systems. At Clabby Analytics, we Believe that, over the next several years, hundreds of new hybrid coprocessor products will come to market – bringing new innovations and new performance deltas along with them. The comparison is shown in Table 1.

VII. PERFORMANCE COMPARISON

	Intel Xeon E5-2697v2	**powers8**
Processor speed	2.697 GHZ	4.15 GHZ
Cores(singale socket)	12	12
Threads/core	2	8
Max main memory	768G	1Tb
Memory controllers	1	2
Level 1	32Kbi+32kbD/core	64 kb/core
Level 2	256KB/core	512KB/core
Level 3	30MB/chip	96MB/chip
Memory bandwidth	59.7GB/s	230GB/s

We compared the computation times of the test application on both processors, excluding the random number generation as shown in Figure 2. The test swaption portfolio consists of 15 trades and 80 forward LIBOR rates are simulated. Thus the portfolio's price and 80 Greek values are calculated below is a plot of the relative performance of Haswell vs. POWER8 – for single and double precision.

Table 1: Comparison between Intel and Power 8

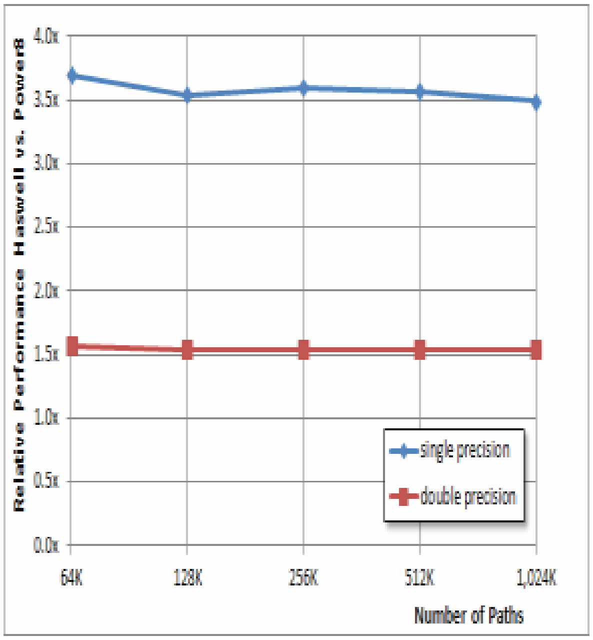


Figure 2: Comparison in terms of Performance

VIII. CONCLUSION

In this paper, we made a comparison between various Intel microprocessors. We briefly explain the history and various categories and also evaluate them based on their performance. Not so long ago, processors were judged largely by raw clock speed alone, a measure of how many calculations the chip is capable of performing in the space of a second. These days, it's all about cores, which have allowed chipmakers like Intel to boost speed by splitting tasks across a number of processing units that exist on the same die. Coupled with software designed to take advantage of multiple cores, such processors can wind up tackling intensive work faster than ever before.

REFERENCES

[1]. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[2]. M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[3]. Khan, F., & Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[4]. M. A. Jan, P. Nanda and X. He, "Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[5]. Khan, F., Kamal, S. A., & Arif, F. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA.

[6]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[7]. Q. Jabeen, F. Khan, S. Khan and M.A Jan. (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. *in the Journal Applied, Environmental, and Biological Sciences (JAEBS*), vol. 6(4S), pp. 82-92. Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[8]. Khan, F., & Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.

[9]. Khan, F. (2014). Secure Communication and Routing Architecture in Wireless Sensor Networks. the 3rd Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.

[10]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" Computer Networks, Vol. 74, PP-92-102, 2014.

[11]. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on* (pp. 1-6). IEEE.

[12]. Mian Ahmad Jan and Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[13]. Khan, S., Khan, F., & Khan, S.A.(2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on

Information Technology: Towards New Smart World (NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.

[14]. Khan, F., Khan, S., & Khan, S. A. (2015, October). Performance improvement in wireless sensor and actor networks based on actor repositioning. In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 134-139). IEEE.

[15]. Khan, S., Khan, F., Jabeen. Q., Arif. F., & Jan. M. A. (2016). Performance Improvement in Wireless Sensor and Actor Networks. in the Journal Applied, Environmental, and Biological Sciences Print ISSN: 2090-4274 Online ISSN: 2090-4215

[16]. Mian Ahmad Jan and Muhammad Khan, "Denial of Service Attacks and Their Countermeasures in WSN", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[17]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[18]. Jabeen, Q., Khan, F., Hayat, M.N., Khan, H., Jan., S.R., Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.

[19]. Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Khan, F., " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : http://ijsrset.com/IJSRSET1622210.php

[20]. Khan, F., Jan, SR, Tahir, M., & Khan, S., (2015) Applications, Limitations, and Improvements in Visible Light Communication Systems" In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 259-262). IEEE.

[21]. Syed Roohullah Jan, Khan, F., Muhammad Tahir, Shahzad Khan,, (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", VFAST Transactions on Software Engineering, (Accepted 2016)

[22]. M. A. Jan, "Energy-efficient routing and secure communication in wireless sensor networks," Ph.D. dissertation, 2016.

[23]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Lightweight Mutual Authentication Scheme for IoT Objects," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, "Submitted", 2016.

[24]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application," *Elsevier Future Generation Computer Systems (FGCS)*, "Accepted", 2016.

[25]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream. InTrustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.

[26]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[27]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams.Journal of Computer and System Sciences.

[28]. Puthal, D., & Sahoo, B. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.

[29]. Puthal, D., Sahoo, B., & Sahoo, B. P. S. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw.© 2009-2011 AJSS Journal, 2(1), 18-22.

[30]. M. A. Jan, P. Nanda, M. Usman, and X. He, "PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks*,"* "accepted", 2016.

[31]. M. Usman, M. A. Jan, and X. He, "Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds," *Elsevier Information sciences*, "accepted", 2016.

[32]. Jan, S. R., Khan, F., & Zaman, A. THE PERCEPTION OF STUDENTS ABOUT MOBILE LEARNING AT UNIVERSITY LEVEL. *NO. CONTENTS PAGE NO.*, 97.

[33]. Khan, F., & Nakagawa, K. (2012). B-8-10 Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. *電子情報通信学会ソサイエティ大会講演論文集*, *2012*(2), 152.

[34]. Safdar, M., Khan, I. A., Ullah, F., Khan, F., & Jan, S. R. Comparative Study of Routing Protocols in Mobile Adhoc Networks.

[35]. Shahzad Khan, Fazlullah Khan, Fahim Arif, Qamar Jabeen, M.A Jan and S. A Khan (2016). "Performance Improvement in Wireless Sensor and Actor Networks", Journal of Applied Environmental and Biological Sciences, Vol. 6(4S), pp. 191-200, Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[36]. M. Usman, M. A. Jan, X. He and P. Nanda, "Data Sharing in Secure Multimedia Wireless Sensor Networks," *in 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16)*, "accepted", 2016.

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 489 – 494, 2016, ISSN: - 2319-8656

5G Wireless Technology- An overview of the current Trends

Muhammad Irfan[1], Jan Sher[1], Naveed Ullah[1], Muhammad Sulaiman[1], Junaid Saleem[1]
[1]Department of computer science, Abdul Wali Khan University Mardan, KPK, Pakistan

Abstract- 5G Wireless technology networks or 5th Generation wireless systems which is used for videos and audios communication announcement the next major time period of mobile telecommunications Criterions time the current next Generation mobile networks confederated .in this paper we are studying different Technologies in 5G The handover of 5G the Models of 5G its architecture, its different components and METIS Task Force Networks. 2-Day video recording is available. Its components access/backhaul integration, direct device-to-device communication, flexible duplex, flexible spectrum usage multi-antenna transmission, ultra-lean design, user/control separation architecture of 5G is highly advanced, its network elements and various terminals are characteristically upgraded to afford a new situation. Likewise, service providers can implement the advance technology to adopt the value-added services easily.

Keywords: Cellular Technology, Wireless Communication, 5th Generation

I. INTRODUCTION

In 2008, the South Korean IT R&D program of "5G mobile communication systems based on beam-division multiple access and relays with group cooperation" was formed. In 2012, the UK Government announced the establishment of a 5G Innovation Centre at the University of Surrey – the world’s first research center set up specifically for 5G mobile researches. In 2012, NYU WIRELESS was established as a multidisciplinary research center, with a focus on 5G wireless researches, as well as its use in the medical and computer-science fields. The center is funded by the National Science Foundation and a board of 10 major wireless companies (as of July 2014) that serve on the Industrial Affiliates board of the center. NYU WIRELESS has conducted and published channel measurements that show that millimeter wave frequencies will be viable for multi-gigabit-per-second data rates for future 5G networks.

In 2012, the European Commission, under the lead of Neelie Kroes, committed 50 million euros for research to deliver 5G mobile technology by 2020. In particular, 5G is the fifth-generation wireless broadband cellular technology which is based on the IEEE802.11ac standard. At least, that’s what the wireless companies envision for the future of mobile. While many parts of the world are still awaiting the rollout of 4G networks, the telecom industry is already looking ahead to the next generation of cellular technology, called 5G. 5G radio access technology will be a key component of the Networked Society [1-3]. It will address high traffic growth and increasing demand for high-bandwidth connectivity. It will also support massive numbers of connected devices and meet the real-time, high-reliability communication needs of mission-critical applications. 5G will provide wireless connectivity for a wide range of new applications and use cases, including wearables, smart homes, traffic safety/control, critical infrastructure, industry processes and very-high-speed media delivery. As a result, it will also accelerate the development of the Internet of Things (IoT) [17-23]. The overall aim of 5G is to provide ubiquitous connectivity for any kind of device and any kind of application that may benefit from being connected. 5G networks will not be based on one specific radio-access technology. Rather, 5G is a portfolio of access and connectivity solutions addressing the demands and requirements of mobile communication beyond 2020 [4-8].

The first 5G wireless channel models have been published. A group of eight partners of the METIS Task Force completed work, and published the first 'interim' 5G channel models officially accepted by the METIS community. METIS, an Integrated Project under the European Union Seventh Framework Program (FP7) for research and development, counts as members 29 key mobile industry players and it is a major large-scale global research activity on 5G. These interim channel models were presented for the first time to the 5G technical community at the Brooklyn 5G Summit which IEEE ComSoc partnered with Ted Rappaport. Actual documentation of the models is available at METIS website and they appear to cover channel models for 2.3 GHz, 2.6 GHz, 5.25 GHz, 26.4 GHz, and 58.68 GHz. The 5G architecture main concentrated on three aspects namely flexibility, scalability and service oriented management. These three aspects are interrelated to each other.

II. DIFFERENT 5G MODELS

5G continues to generate buzz and grab the efforts and the attention of many of us in the Communications Technology Industry. The interest of IEEE ComSoc members is such that, for example, 7 out of the top-10 most downloaded papers in May are 5G related. The May 2014 special issue of the IEEE CTN on 5G brought our readers up to date on the current state of 5G technology. Just a few weeks later, with the rapid research progress and industry interest in the topic, an update is due. News of preliminary 5G wireless channel models, reports of 5G live network test results, renewed focus in emerging architectures, and evaluation and plans for the impact of 5G are the key topics in this update. Let's get to the details.

A. First prototype of 5G Model

A group of eight partners of the METIS Task Force completed work, and published the first 'interim' 5G channel models officially accepted by the METIS community. METIS, an Integrated Project under the European Union Seventh Framework Programme (FP7) for research and development, counts as members 29 key mobile industry players and it is a major large-scale global research activity on 5G. These interim channel models were presented for the first time to the 5G technical community at the Brooklyn 5G Summit which IEEE ComSoc partnered with Ted Rappaport from NYU WIRELESS and Amitabha Ghosh from Nokia Solutions and Networks. 2-Day video recording available. Actual documentation of the models is available at METIS website and they appear to cover channel models for 2.3 GHz, 2.6 GHz, 5.25 GHz, 26.4 GHz, and 58.68 GHz.

B. Speed of 5G in Live Test Network

The benchmark came from Ericsson that reported in its website achieving 5 Gbps speed in live test of pre standard 5G, using an innovative new radio interface concept in combination with advanced Multiple-Input Multiple-Output (MIMO) technology with wider bandwidths, higher frequencies and shorter transmission time intervals. As far as frequency, the 5G test network used a 15 GHz frequency band, which is higher and shorter range than current 3G/4G cellular frequencies that top out at around 2.6 GHz, i.e. 2600 MHz LTE Band 7. The choice of short-range would make deployments of this technology suitable for densely populated urban areas, where many base stations could be deployed to offer super-fast speeds over a small area.

C. D2D Technology of 5G Architecture Model

There has been much interest in applying Device-2-Device (D2D) principles to public safety and proximity based services. Because of the high profile of this topic, IEEE ComSoc Communications Magazine July 2014 issue and Wireless Communications Magazine June 2014 issue feature several articles where IEEE ComSoc experts and industry leaders exciting area of D2D and has summarized its recent findings in use cases, design approaches and performance aspects. The common thread in these D2D articles is an ongoing need/interest in expanding the definition of heterogeneous cellular networks to include D2D capabilities with location, performance and capacity gains [9-16].

We are still in the early stages of defining 5G. There are different visions and a range of proposed solutions. How do we know if those visions and solutions meet the needs of millions of people and billions of connected devices? The European Commission's Directorate-General for Communications Networks, Content, and Technology wants to learn about these unknowns issuing a 5G introduction in Europe—SMART 2014/0008 call for tenders to gather data for the Strategic Planning of 5G Introduction in Europe aim to help plan the critical phases for 5G mobile wireless systems deployment [24-28], from the research and innovation activities to infrastructure investments and prospects for early commercial developments.

III. 5G NETWORK ARCHITECTURE

The 5G architecture main concentrated on three aspects namely flexibility, scalability and service oriented management. These three aspects are interrelated to each other to drive the 5G technology to fulfill the various requirements in the network flexibility. The architecture will be flexible enough to handle the requirements of the use case service. Scalability will assist by flexibility to fulfil the requirements of the services. The new generation of RAN networks needs to be efficiently handled multiple layers and a variety of air interfaces in the access and the backhaul domains. They have to control the dynamic traffic, user behavior, and active nodes involved. This need to be able to differentiate a larger variety The operators with both fixed and mobile network infrastructure cost reduction is a grater improvement in the 5G technology. Reuse of network infrastructure on transport and access layer (Fixed mobile convergence (FMO)) against SDN/NFV is seen as enables to allow multi-operator network infrastructure and resource sharing. The architecture will provide the necessary flexibility to realize efficient integration and cooperation of functional block [29-33] according to individual service. The function can be flexibly modified, tailor and created by the function co-coordinator according to the dataflow and can be moved to the relevant network demand.

The architecture is based on WSDN approach to enables on demand creation of customized virtual networks using shared resources and effective service adaptive decoupling of control and data plane in order to provide routing and mobility management as shown in Figure 1. When compared to present 4G certain functionalities of the user equipment's may be partially controlled by the operator

[34-36]. The flexibility may be limited by capabilities of the network such as sensors, which may not be updated with all new functionalities.

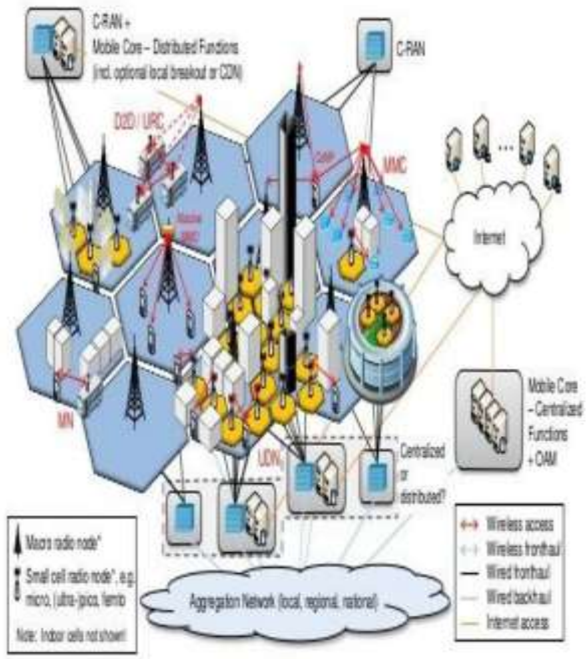

C-RAN +
Mobile Core – Distributed Functions
(incl. optional local breakout or CDN)
C-RAN
D2D / URC
MMC
Internet
Mobile Core
– Centralized
Functions
+ OAM
MN
UDN
Centralized
or
distributed?
Macro radio node*
Small cell radio node*, e.g.
micro, (ultra-)pico, femto
Note: Indoor cells not shown!
Aggregation Network (local, regional, national)
Wireless access
Wireless fronthaul
Wired fronthaul
Wired backhaul
Internet access

Figure 1: Architecture of 5G Technology

IV. Components of 5G

The architecture model of 5G consists of the following main components.

A. Phantom Cell

Network densification using small cells with low power nodes is promising solution with mobile traffic explosion, especially in high traffic area (hot spot area). These cells develop advanced centralized RAN (C-RAN) architecture for commercial use. Advanced C-RAN adopts the centralized network architecture with many branches of remote radio equipment (RRE) and utilizes LTE advanced carrier aggregation (CA) functionality between macro and small cell carrier. CA functionality help to maintain the connectivity and mobility under the macro cell coverage while small cells called „Add-on‟ cells achieve higher throughput performance and larger capacity. The advanced C-RAN architecture handles all processing for CA and handover within a centralized baseband unit (BBU) at eNodeB, which drastically reduces the amount of signaling to the core network. The "Phantom cell" concept is based on a multi-layer network architecture, which spills the control (C) plane and user data (U) plane between macro cell and small cell using different frequency bands The major benefits of the phantom cell architecture are similar to those of advanced C-RAN architecture for LTE-Advanced, which include enhanced capacity by small cell, easy deployment of higher frequency bands. The concept of phantom cell architecture includes advanced functionalities such as inter node aggregation, relaxed backhauling and signaling requirements and enhanced small cell discovery. 5G concept user Phantom cell architecture as the baseline which to integrate future multilayer networks using lower and high frequency bands.

B. Access/Backhaul Integration

Wireless technology is already frequently used as part of the backhaul solution. Such wireless-backhaul solutions typically operate under line-of-sight conditions using proprietary radio technology in higher frequency bands, including the millimeter wave (mmW) band.

In the future, the access (base-station-to-device) link will also extend to higher frequencies. Furthermore, to support dense low-power deployments, wireless backhaul will have to extend to cover non-line-of-sight conditions, similar to access links. In the 5G era, the wireless-access link and wireless backhaul should not therefore be seen as two separate entities with separate technical solutions. Rather, backhaul and access should be seen as an integrated wireless-access solution able to use the same basic technology and operate using a common spectrum pool. This will lead to more efficient overall spectrum utilization as well as reduced operation and management effort.

C. Device-To-Device Communication

The possibility of limited direct device-to-device (D2D) communication has recently been introduced as an extension to the LTE specifications. In the 5G era, support for D2D as part of the overall wireless-access solution should be considered from the start. This includes peer-to-peer user-data communication directly between devices, but also, for example, the use of mobile devices as relays to extend network coverage. D2D communication in the context of 5G should be an integral part of the overall wireless-access solution, rather than a stand-alone solution. Direct D2D communication can be used to offload traffic, extend capabilities and enhance the overall efficiency of the wireless-access network. Furthermore, in order to avoid uncontrolled interference to other links, direct D2D communication should be under network control. This is especially important for the case of D2D communication in licensed spectrum.

D. Flexible Duplex Communication

Frequency Division Duplex (FDD) has been the dominating duplex arrangement since the beginning of the mobile communication era as shown in Figure 2. In the 5G era, FDD will remain the main duplex scheme for lower frequency bands. However, for higher frequency bands – especially above 10GHz – targeting very dense deployments, In very dense deployments with low-power nodes, the TDD-specific interference scenarios (direct base-station-to-base-station and device-to-device interference) will be similar to the 'normal' base-station-to-device and device-to-base-station interference that also occurs for FDD. Furthermore, for the dynamic traffic variations expected in very dense deployments, the ability to dynamically assign transmission resources (time slots) to different transmission directions may allow more efficient utilization of the available spectrum. To reach its full potential, 5G should therefore allow for very flexible and dynamic assignment of TDD transmission resources. This is in contrast to current TDD-based mobile technologies, including TD-LTE, for which there are restrictions on the downlink/uplink configurations, and for which there typically exist assumptions about the same configuration for neighbor cells and also between neighbor operators.

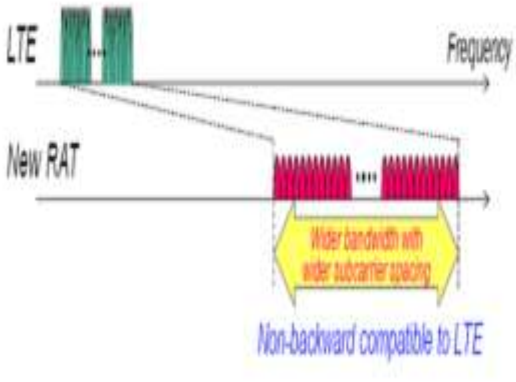

LTE
Frequency
New RAT
Wider bandwidth with wider subcarrier spacing
Non-backward compatible to LTE

Figure 2: Flexible Duplex Communication

V. CONCLUSION

5G is the next step in the evolution of mobile communication and will be a key component of the Networked Society. In particular, 5G will accelerate the development of the Internet of Things. To enable connectivity for a wide range of applications and use cases, the capabilities of 5G wireless access must extend far beyond those of previous generations of mobile communications. These capabilities include very high achievable data rates, very low latency and ultra-high reliability. Furthermore, 5G wireless access needs to support a massive increase in traffic in an affordable and sustainable way, implying a need for a dramatic reduction in the cost and energy consumption per delivered bit. 5G wireless access will be realized by the evolution of LTE for existing spectrum in combination with new radio access technologies that primarily target new spectrum. Key technology components of 5G wireless access include access/backhaul integration, device-to-device communication, flexible duplex, flexible spectrum usage, multi-antenna transmission, ultra-lean design, and user/control separation.

REFERENCES

[1]. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[2]. M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[3]. Khan, F., & Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[4]. M. A. Jan, P. Nanda and X. He, "Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[5]. Khan, F., Kamal, S. A., & Arif, F. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA.

[6]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[7]. Q. Jabeen, F. Khan, S. Khan and M.A Jan. (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. *in the Journal Applied, Environmental, and Biological Sciences (JAEBS*), vol. 6(4S), pp. 82-92. Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[8]. Khan, F., & Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.

[9]. Khan, F. (2014). Secure Communication and Routing Architecture in Wireless Sensor Networks. the 3rd Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.

[10]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" Computer Networks, Vol. 74, PP-92-102, 2014.

[11]. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on* (pp. 1-6). IEEE.

[12]. Mian Ahmad Jan and Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[13]. Khan, S., Khan, F., & Khan, S.A.(2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.

[14]. Khan, F., Khan, S., & Khan, S. A. (2015, October). Performance improvement in wireless sensor and actor networks based on actor repositioning. In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 134-139). IEEE.

[15]. Khan, S., Khan, F., Jabeen. Q., Arif. F., & Jan. M. A. (2016). Performance Improvement in Wireless Sensor and Actor Networks. in the Journal Applied, Environmental, and Biological Sciences Print ISSN: 2090-4274 Online ISSN: 2090-4215

[16]. Mian Ahmad Jan and Muhammad Khan, "Denial of Service Attacks and Their Countermeasures in WSN", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[17]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[18]. Jabeen, Q., Khan, F., Hayat, M.N., Khan, H., Jan., S.R., Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.

[19]. Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Khan, F., " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : http://ijsrset.com/IJSRSET1622210.php

[20]. Khan, F., Jan, SR, Tahir, M., & Khan, S., (2015) Applications, Limitations, and Improvements in Visible Light Communication Systems" In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 259-262). IEEE.

[21]. Syed Roohullah Jan, Khan, F., Muhammad Tahir, Shahzad Khan,, (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", VFAST Transactions on Software Engineering, (Accepted 2016)

[22]. M. A. Jan, "Energy-efficient routing and secure communication in wireless sensor networks," Ph.D. dissertation, 2016.

[23]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Lightweight Mutual Authentication Scheme for IoT Objects," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, "Submitted", 2016.

[24]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application," *Elsevier Future Generation Computer Systems (FGCS)*, "Accepted", 2016.

[25]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream. InTrustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.

[26]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[27]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams.Journal of Computer and System Sciences.

[28]. Puthal, D., & Sahoo, B. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.

[29]. Puthal, D., Sahoo, B., & Sahoo, B. P. S. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw.© 2009-2011 AJSS Journal, 2(1), 18-22.

[30]. M. A. Jan, P. Nanda, M. Usman, and X. He, "PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks*,"* "accepted", 2016.

[31]. M. Usman, M. A. Jan, and X. He, "Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds," *Elsevier Information sciences*, "accepted", 2016.

[32]. Jan, S. R., Khan, F., & Zaman, A. THE PERCEPTION OF STUDENTS ABOUT MOBILE LEARNING AT UNIVERSITY LEVEL. *NO. CONTENTS PAGE NO.*, 97.

[33]. Khan, F., & Nakagawa, K. (2012). B-8-10 Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. *電子情報通信学会ソサイエティ大会講演論文集*, *2012*(2), 152.

[34]. Safdar, M., Khan, I. A., Ullah, F., Khan, F., & Jan, S. R. Comparative Study of Routing Protocols in Mobile Adhoc Networks.

[35]. Shahzad Khan, Fazlullah Khan, Fahim Arif, Qamar Jabeen, M.A Jan and S. A Khan (2016). "Performance Improvement in Wireless Sensor and Actor Networks", Journal of Applied Environmental and Biological Sciences, Vol. 6(4S), pp. 191-200, Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[36]. M. Usman, M. A. Jan, X. He and P. Nanda, "Data Sharing in Secure Multimedia Wireless Sensor Networks," *in 15th IEEE International Conference on Trust, Security and Privacy in Computing and*

Communications (IEEE TrustCom-16), “accepted”, 2016.

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 495 – 499, 2016, ISSN: - 2319-8656

Moore’s Law Effect on Transistors Evolution

Sabeen Rashid[1], Rabia Shakeel[1], Huma Bashir[1], Khadija Malik[1], Kainat Wajib[1]
[1]Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan

Abstract-With respect to time increasing in the number of transistors has a great effect on the performance and the speed of processors. In this paper we are comparing the transistors evolution related to Moore’s law. According to the Moore’s law the number of transistors should be double every 24 month. The effect of increasing processors design complexity also increases the power consumption and cost of design efforts. In this paper we discuss the methods and procedures to scale the hardware complexity of processors.

Keywords: Hardware Complexity, Processor Design, Transistor Count, Moore’s Law.

I. INTRODUCTION

The MOORE’s law observations states that the number of transistors are doubling every two years. More precisely within the period of “18 months” is due to Intel executive David House, the increase in number of transistors and increase in speed of transistors give rise to the effect of increase in the performance of the transistors. Moore’s law has its same effect during the history of semiconductor since the advent of computing devices to now mobile devices, a continuous improvement of silicon chips [1-6]. The two factors have made a great impact on the success of Moore’s law, consumers demand for more functionality and the competition among the developers.
The technology has improved, better to call it as evaluated from mid-1970’s 6800 processor with 5000 transistors to the today’s multicore processors like reaching the limit of 3 billion. The fact about Moore’s law is to improve those area that helps to achieve the more and more small sized transistors and with more better technology

II. BACKGROUND

Moore's law state that transistor numbers become two times in every 18 to 24 months in article. "Cramming more components onto integrated circuits", *Electronics Magazine* 19 April 1965: The transistor cost has become double in every 24 months and this is remaining increasing at least at this order, if no chance of increase more. For many years of gap the speed of increase became very low so we can say that there are no observable changes in period of 10 years. During the year of 1975 the transistor cost on each integrated circuit is atleast 65000. So clearly I am sure about that one wafer can adjust one integrated circuit [2]. The statement of Moore’s that number of transistor on integrated circuit will becomes two times in a period of every 18 to 24 months. The statement is given by scientist named as Golden Moore in 1965. The law is still useful and applicable. It is the high demand of small sized, low Power consumption and higher processing speed transistors that have prolonged the life of Moore’s Law, and until now Moore’s Law is still used as the guideline for transistor manufacturing. The Moore’s Law graph is shown in Figure 1.

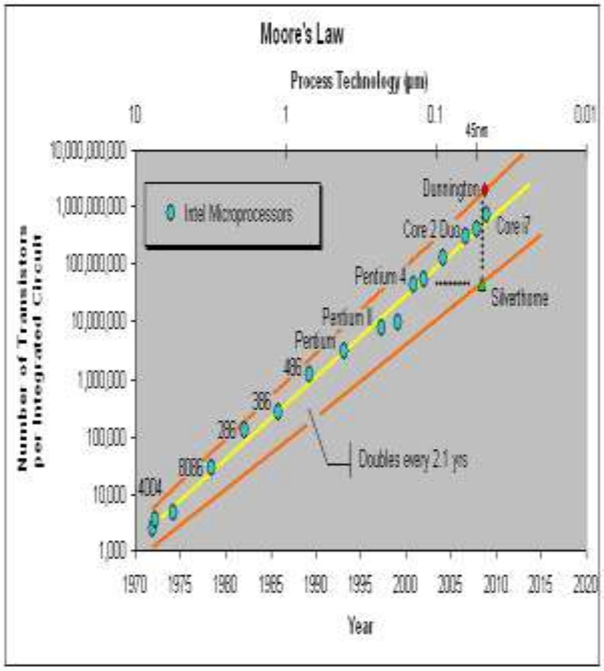


Figure 1.Moore’s Law Graph

During the period of 1970s more electronics were built as compared to the previous years as industry was more than doubling the total number of transistors. The transistors capacity has continuously getting better. Moore’s law rating has recently slowed but still on a good growth. Todays a number of transistors in one year is up to 10^18. According to a well-known naturalist Edward O. Wilson, at Harvard, had counted that they were approximately10^16 and 10^17 ants on earth. In 1990s then the semiconductor industry was producing a transistor for every ant. Now, the poor little ant has to carry a hundred of them [7-9] around if he is going to get his share.

Processor speeds from the 1970's to 2009 and then again in 2010, one may think [10-19] that the law has reached its limit or is nearing the limit. In the 1970's processor speeds ranged from 740 KHz to 8MHz; notice that the 740 is KHz, which is Kilo Hertz – while the 8 is MHz, which is Mega Hertz.

From 2000 – 2009 there has not really been much of a speed difference as the speeds range from 1.3 GHz to 2.8 GHz, which suggests that the speeds have barely doubled within a 10 year span. This is because we are looking at the speeds and not the number of transistors; in 2000 the number of transistors in the CPU numbered 37.5 million, while in 2009 the number went up to an outstanding 904 million; this is why it is more accurate to apply the law to transistors than to speed [20].

From all of the above discussion about transistors ,every computer literate person can't drawn result from it easily [21-25] so we say that earlier processors used one CPU while todays processors are multicore technology using more than one CPU,s.

In example above the speed of the CPU during many years of gap increase from 1.3 to 2.8 which is speed of a single CORE , QUAD CORE processsors.in conclusion we can say that power of 2.8 is obtain if multiply it with four which is 11.2 this is very large from 1.3.

III. CHALLENGES INCURRED

There is an inflection point to the technology of semiconductors. Table 1 below, shows some serious challenges faced by semiconductor technology .More and smaller transistors are not always "better". Second denard scaling also has ended, power per transistor is not good [26-33]. Third, challenge is fabrication variations subject to the reliability of transistors (nano-scale features e.g., gate oxides only atoms thick). Fourth, communication among computation elements must be managed through locality to achieve goals at acceptable cost and energy with new opportunities (e.g., chip stacking) and new challenges (e.g., data centers). Fifth, for achieving high performance, costs to create, design, verify, fabricate, and test are growing, making them harder to afford.

Table 1: Technology's Challenges to Computer Architecture

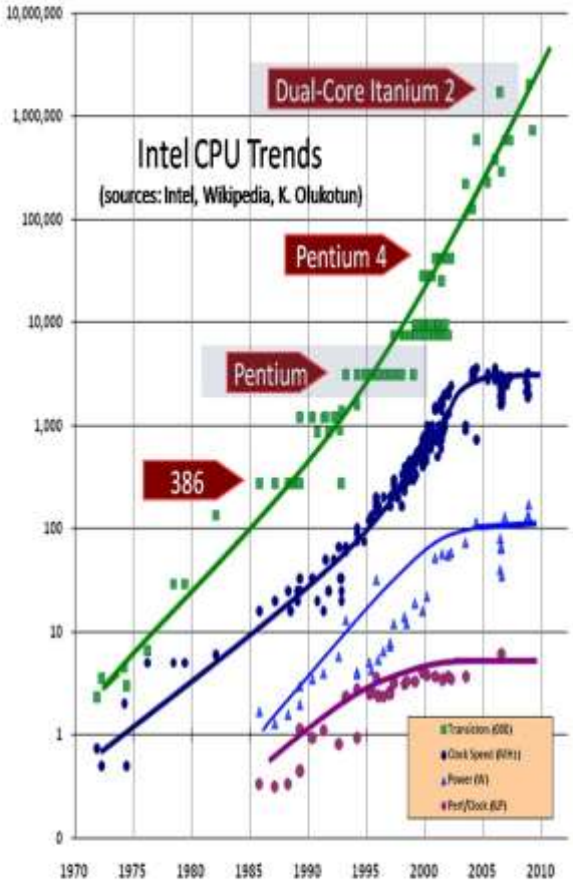
1970s	Newer trend
Double transistors per chip_ in every 18-24 months	Transistor count still 2× every 18-24 months,
Dennard Scaling(power per transistor) — near-constant power/chip	Not viable for power/chip to double (with 2× transistors/chip growth)
The modest levels of transistor unreliability easily hidden (e.g., via ECC)	Transistor reliability is going to be effected
Focus on computation over communication	Restricted communication communication more expensive than computation
One-time creation of very high performance and reliability is difficult	Expensive to design, verify, fabricate, and test

IV. INCREASING THE NUMBER OF TRANSISTORS

Many limitations are still there, such as increasing the density size, the die size, physical size decrement, the voltage [34].

Since the surface area of a transistor determines the transistor count per square millimeter of silicon, and as the feature size is decreasing transistors density increases quadratically. And as the surface area of a transistor determines the transistor count per square millimeter of silicon [35]. The increase in transistor performance is more complicated As the physical size is decreased. A reduction in operating voltage to maintain correct operation and reliability of the transistor is required in the vertical dimension shrink. This combination [36-39] of scaling factors leads to a complex interrelationship between the transistor performance and the process feature size and it makes difficult to apply Moore's Law in the future. Some studies have shown that physical limitations could be reached by 2018 [7] or 2020-2022[8, 9, 10, 11].

Processor's hardware complexity is caused by doubling the number [40-47] of transistors every two years (see Table 2), which will be limited after a few years [12, 13, 14, 15].



V. CONCLUSION

Although clock speeds and transistors per circuit have not kept pace with the original exponential forecast known as Moore's Law, doubling every year, computing performance and cost efficiencies continue to advance at a remarkable pace. Competition among the major processor manufacturers, Intel, AMD, IBM, Sun, and Texas Instruments can be expected to push the industry down the long-run average total cost curves described by Gordon Moore in 1965. As he predicted, the result will be dramatic improvements and much lower prices for computing performance. While clock speeds may continue to be a standard measure of performance.

REFERENCE

[1]. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[2]. M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[3]. Khan, F., & Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[4]. M. A. Jan, P. Nanda and X. He, "Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[5]. Khan, F., Kamal, S. A., & Arif, F. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA.

[6]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[7]. Q. Jabeen, F. Khan, S. Khan and M.A Jan. (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. *in the Journal Applied, Environmental, and Biological Sciences (JAEBS*), vol. 6(4S), pp. 82-92. Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[8]. Khan, F., & Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.

[9]. Khan, F. (2014). Secure Communication and Routing Architecture in Wireless Sensor Networks. the 3rd Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.

[10]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" Computer Networks, Vol. 74, PP-92-102, 2014.

[11]. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on* (pp. 1-6). IEEE.

[12]. Mian Ahmad Jan and Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[13]. Khan, S., Khan, F., & Khan, S.A.(2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on Information Technology: Towards New Smart World

(NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.

[14]. Khan, F., Khan, S., & Khan, S. A. (2015, October). Performance improvement in wireless sensor and actor networks based on actor repositioning. In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 134-139). IEEE.

[15]. Khan, S., Khan, F., Jabeen. Q., Arif. F., & Jan. M. A. (2016). Performance Improvement in Wireless Sensor and Actor Networks. in the Journal Applied, Environmental, and Biological Sciences Print ISSN: 2090-4274 Online ISSN: 2090-4215

[16]. Mian Ahmad Jan and Muhammad Khan, "Denial of Service Attacks and Their Countermeasures in WSN", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[17]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[18]. Jabeen, Q., Khan, F., Hayat, M.N., Khan, H., Jan., S.R., Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.

[19]. Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Khan, F., " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : http://ijsrset.com/IJSRSET1622210.php

[20]. Khan, F., Jan, SR, Tahir, M., & Khan, S., (2015) Applications, Limitations, and Improvements in Visible Light Communication Systems" In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 259-262). IEEE.

[21]. Syed Roohullah Jan, Khan, F., Muhammad Tahir, Shahzad Khan,, (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", VFAST Transactions on Software Engineering, (Accepted 2016)

[22]. M. A. Jan, "Energy-efficient routing and secure communication in wireless sensor networks," Ph.D. dissertation, 2016.

[23]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Lightweight Mutual Authentication Scheme for IoT Objects," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, "Submitted", 2016.

[24]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application," *Elsevier Future Generation Computer Systems (FGCS)*, "Accepted", 2016.

[25]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream. InTrustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.

[26]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[27]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams.Journal of Computer and System Sciences.

[28]. Puthal, D., & Sahoo, B. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.

[29]. Puthal, D., Sahoo, B., & Sahoo, B. P. S. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw.© 2009-2011 AJSS Journal, 2(1), 18-22.

[30]. M. A. Jan, P. Nanda, M. Usman, and X. He, "PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks,*"* "accepted", 2016.

[31]. M. Usman, M. A. Jan, and X. He, "Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds," *Elsevier Information sciences*, "accepted", 2016.

[32]. Jan, S. R., Khan, F., & Zaman, A. THE PERCEPTION OF STUDENTS ABOUT MOBILE LEARNING AT UNIVERSITY LEVEL. *NO. CONTENTS PAGE NO.*, 97.

[33]. Khan, F., & Nakagawa, K. (2012). B-8-10 Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. *電子情報通信学会ソサイエティ大会講演論文集*, *2012*(2), 152.

[34]. Safdar, M., Khan, I. A., Ullah, F., Khan, F., & Jan, S. R. Comparative Study of Routing Protocols in Mobile Adhoc Networks.

[35]. Shahzad Khan, Fazlullah Khan, Fahim Arif, Qamar Jabeen, M.A Jan and S. A Khan (2016). "Performance Improvement in Wireless Sensor and Actor Networks", Journal of Applied Environmental and Biological Sciences, Vol. 6(4S), pp. 191-200, Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[36]. M. Usman, M. A. Jan, X. He and P. Nanda, "Data Sharing in Secure Multimedia Wireless Sensor Networks," *in 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16)*, "accepted", 2016.

[37]. "Moore's Law to roll on for another decade" (http://news.cnet.com/2100-1001-984051.html). . Retrieved 2011-11-27. "Moore also affirmed he never said transistor count would double every 18 months, as is commonly said. Initially, he said transistors on a chip would double every year. He then recalibrated it to every two years in 1975. David House, an Intel

executive at time, noted that the changes would cause computer performance to double every 18 months.

[38]. Moore, Gordon E. (1965). "Cramming more components onto integrated circuits" (http://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore1965_Article.pdf) (PDF). Electronics Magazine. p. 4. . Retrieved 2006-11-11`

[39]. Robert W. Keyes, "Physical limits of silicon transistors and circuits", September 2005.

[40]. F. Morals, L. Torres, M. Robert, D. Auvergne, "Estimation of layout densities for CMOS digitalcircuits", Proceeding International Workshop on Power and Timing Modeling Optimization Simulation (PATMOS'98), pp. 61-70, November 1998, Lyngby, Danemark.

[41]. John L. Hennessy and David A. Patterson, "Computer Architecture, A Quantitative Approach", 5thed., pp. 17-26, 2011.

[42]. Jan M. Rabaey, "Design at the end of Silicon Roadmap", Keynotes Address III, University ofCalifornia, Berkelev, IEEE, ASP-DAC 2005.

[43]. Ahmad, Khaled; Schuegraf, Klaus, "Transistor Wars: Rival architecture face off in a bid to keep Moore's Law-alive", IEEE Spectrum: 50, November 2011.

[44]. Brooke Crothers, "End of Moore's Law: it's not just about physics", August 28, 2013.

[45]. Robert Colwell, "The Chip Design Game at the End of Moore's Law", Hot Chips, August 2013.http://news.cnet.com/8301-1001_3-57600373-92/end-of-moores-law-its-not-just-about-physics/

[46]. Joel Hruska, "Intel's former chief architect: Moore's law will be dead within a decade", August 30, 2013.

[47]. Pradip Bose David H. Albonesi Diana Marculescu, "Complexity-Effective Design", Proceeding International Workshop on Complexity-Effective Design, Madison, Wisconsin, June 5, 2005.

International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 500 – 503, 2016, ISSN: - 2319-8656

Comparative Study of RISC AND CISC Architectures

Shahzeb[1], Naveed Hussain[1], Amanulllah[1], Furqan Ahmad[1], Salman Khan[1]
[1]Department of Computer Science, Abdul Wali Khan University Mardan, KPK, Pakistan

Abstract- Comparison between RISC and CISC in the language of computer architecture for research is not very simple because a lot of researcher worked on RISC and CISC Architectures. Both these architecture differ substantially in terms of their underlying platforms and hardware architectures. The type of chips used differs a lot and there exists too many variants as well. This paper gives us the architectural comparison between RISC and CISC architectures. Also, we provide their advantages performance point of view and share our idea to the new researchers.

Keywords: RISC, CISC, Architecture, AMD

I. INTRODUCTION

The Microprocessor chips are divided into two categories. In both of these architectures the main purpose is to optimal the performance of the system. Our Research on these two architecture which is complex but we do our best [1-8]. CISC is stand for complex instruction set computer. Nowadays the PCs mostly uses CISC architecture Like AMD and Intel etc. CISC chips have large and complex instructions [9-13]. We know that hardware is faster than software so therefore one should make a powerful instruction set which provides programmers with assembly instructions to do a lot with short program. In common CISC chips are relatively slow (as compared to RISC).

RISC is stand for Reduced Instruction Set Computer. Nowadays mostly Mobile Phones Based on RISC architecture Like MIPS and ARM etc. RISC has simple and small Instruction. RISC chips Comes around the mid 80's because the reaction of CISC chips. The philosophy behind that almost no one use complex instructions and mostly people uses compilers which never use complex instructions. So for Apple uses RISC chips [14-20]. So therefore simple and faster instructions are better than large complex and slower (CISC) instructions. However, RISC required more instruction to complete a task than CISC. An advantage of RISC is that because it more simple instructions. RISC chips require less transistors which makes easier to design and cheaper to produce. So now it easier to write powerful optimal compilers since fewer instructions exists.

II. COMPARISON OF RISC AND CISC

First we explain the properties of CISC architectures and then we explain the properties of RISC architecture.

Properties of CISC:

1. Some simple and very complex instructions
2. In CISC instructions take more than 1 clock per Cycle to execute
3. Variable size instructions
4. No pipelining
5. Few registers
6. Not a load and store machine
7. For Compilation not so good in term of speed
8. Emphasis of Hardware
9. Transistors are used for storing complex instructions

Properties of RISC:

1. Small and simple instructions
2. In RISC Instructions are execute in one clock cycle per Instructions
3. All instructions have the same length
4. Load and Store architecture implemented due to the desired single-cycle operation
5. Have Pipelining
6. More register than CISC
7. Optimal compilation speed as compared to CISC
8. Emphasis on software
9. Compare to CISC a RISC Spends more transistors on memory registers

Examples of CISC and RISC Processors are shown in Table 1.

Table 1: RISC and CISC Architecture

CISC	**RISC**
IBM 370-169	MIPS R2000
VAX 11-780	SUN SPARC
MICROVAX 2	INTEL i860
INTEL 80386	MOTOROLA 8800
INTEL 80286	POWERPC 601

A. ADVANTAGES OF RISC:

Implementation with simple instructions provides many advantages over implementing as compared to CISC Processors. Simple instruction set allow for pipeline superscalar designing RISC processor often achieved two to four times performance of CISC processors using [21-27] comparable semiconductor technology and similar clock rates.

Simple hardware. Because instructions set of a (RISC) processor is so simple, it uses up much less chips spaces and extra functions i.e. memory management unit or floating point arithmetic units, can also be placed on the similar chip. Smaller chips allows a semiconductor manufacturers to placed more parts on single silicon wafer which can lower per chips cost dramatically and have short design cycles. Since RISC processors are simpler than corresponding CISC processors they can be design more quickly and take advantage of other technological [28-33] developments sooner than corresponds CISC design leading to great leaps in performance between generations.

B. Advantages of CISC:

At the time of their initial development CISC machines use technologies to optimize the performance of a computer. Microprogramming is easy as assembly Programming language to implement and less expensive than hardwiring a control unit.

The ease of micro coding newly instructions allows designers to make (CISC) machines upwardly compatible new computer run the same programs as early computers because the new computers would contained a superset of instructions of earlier computers. As each instruction became more capable less instruction used to implement the given task. This made efficient uses of the relative slow main memory.

Because micro program instructions set can be write to match the construct of high level languages the compilers doesn't have to be as complicated.

III. PROBLEM STATEMENT

We discussed the RISC and CISC Architectures. Nowadays the Technology is growing rapidly the problem is that how fix the problem of performance between Risc and Cisc to overcome the Comments of different architecture [34-36] who claim the issues of Performance.

IV. PROPOSED IDEA

We study a lot of Research Articles Our statistics is 40 to 50 percent Researchers talk about the same issues. So in our idea is to combine these to Architectures and make a hybrid processor to overcome the problem but it is not so simple it take a lot of time. We call Fresher Students or Professionals to do work on the hybrid processor based on Risc and Cisc which will be helps the designers and developers.

The motivation for the design of RISC processors arose from technological developments which changed gradually the architectural parameters traditionally used in the computer industry. Researchers have already given a detailed account of the prehistory of RISC. At the abstract architectural level the general trend until the middle of the seventies was the design of ever richer instruction sets which could take some of the burden of interpreting high level computer languages from the compiler to the hardware. The philosophy of the time was to build machines which could diminish the semantic gap between high level languages and the machine language. Many special instructions were included in the instruction set in order to improve the performance of some operations and several machine instructions looked almost like their high-level counterparts. If anything was to be avoided it was, first of all, compiler complexity. At the implementation level, microcoding provided a general method of implementing increasingly complex instruction sets using a fair amount of hardware. Microcoding also made possible to develop families of compatible computers which differed only in the underlying technology and performance level, like in the case of the IBM/360 system.

The metrics used to assess the quality of a design corresponded directly to these two architectural levels: the first metric was code density, i.e., the length of compiled programs; the second metric was compiler complexity. Code density should be maximized, compiler complexity should be minimized. Not very long ago Wirth [1986] was still analyzing some microprocessor architectures based exactly on these criteria and denouncing them for being "halfheartedly high-level language oriented."

V. CONCLUSION

In this paper we briefly explain RISC and CISC architectures on the bases of their properties and also explain their advantages. Now Due to this exploration both architectures RISC and CISC have continuously developed. The RISC architecture had advantages that the results to a machines excellent performance and adopted for commercial products. We also talk little bit about the performance problem provide idea for Researchers to further explain the Risc and Cisc and also to Clarify the new Processor based on Risc and Cisc.

REFERENCES

[1]. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[2]. M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[3]. Khan, F., & Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[4]. M. A. Jan, P. Nanda and X. He, "Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[5]. Khan, F., Kamal, S. A., & Arif, F. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA.

[6]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[7]. Q. Jabeen, F. Khan, S. Khan and M.A Jan. (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. *in the Journal Applied, Environmental, and Biological Sciences (JAEBS*), vol. 6(4S), pp. 82-92. Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[8]. Khan, F., & Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.

[9]. Khan, F. (2014). Secure Communication and Routing Architecture in Wireless Sensor Networks. the 3rd Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.

[10]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" Computer Networks, Vol. 74, PP-92-102, 2014.

[11]. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on* (pp. 1-6). IEEE.

[12]. Mian Ahmad Jan and Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[13]. Khan, S., Khan, F., & Khan, S.A.(2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.

[14]. Khan, F., Khan, S., & Khan, S. A. (2015, October). Performance improvement in wireless sensor and actor networks based on actor repositioning. In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 134-139). IEEE.

[15]. Khan, S., Khan, F., Jabeen. Q., Arif. F., & Jan. M. A. (2016). Performance Improvement in Wireless Sensor and Actor Networks. in the Journal Applied, Environmental, and Biological Sciences Print ISSN: 2090-4274 Online ISSN: 2090-4215

[16]. Mian Ahmad Jan and Muhammad Khan, "Denial of Service Attacks and Their Countermeasures in WSN", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[17]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[18]. Jabeen, Q., Khan, F., Hayat, M.N., Khan, H., Jan., S.R., Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.

[19]. Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Khan, F., " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : http://ijsrset.com/IJSRSET1622210.php

[20]. Khan, F., Jan, SR, Tahir, M., & Khan, S., (2015) Applications, Limitations, and Improvements in Visible Light Communication Systems" In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 259-262). IEEE.

[21]. Syed Roohullah Jan, Khan, F., Muhammad Tahir, Shahzad Khan,, (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", VFAST Transactions on Software Engineering, (Accepted 2016)

[22]. M. A. Jan, "Energy-efficient routing and secure communication in wireless sensor networks," Ph.D. dissertation, 2016.

[23]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Lightweight Mutual Authentication Scheme for IoT Objects," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, "Submitted", 2016.

[24]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application," *Elsevier Future Generation Computer Systems (FGCS)*, "Accepted", 2016.

[25]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream. InTrustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.

[26]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[27]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams.Journal of Computer and System Sciences.

[28]. Puthal, D., & Sahoo, B. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.

[29]. Puthal, D., Sahoo, B., & Sahoo, B. P. S. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw.© 2009-2011 AJSS Journal, 2(1), 18-22.

[30]. M. A. Jan, P. Nanda, M. Usman, and X. He, "PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks*,"* "accepted", 2016.

[31]. M. Usman, M. A. Jan, and X. He, "Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds," *Elsevier Information sciences*, "accepted", 2016.

[32]. Jan, S. R., Khan, F., & Zaman, A. THE PERCEPTION OF STUDENTS ABOUT MOBILE LEARNING AT UNIVERSITY LEVEL. *NO. CONTENTS PAGE NO.*, 97.

[33]. Khan, F., & Nakagawa, K. (2012). B-8-10 Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. 電子情報通信学会ソサイエティ大会講演論文集, *2012*(2), 152.

[34]. Safdar, M., Khan, I. A., Ullah, F., Khan, F., & Jan, S. R. Comparative Study of Routing Protocols in Mobile Adhoc Networks.

[35]. Shahzad Khan, Fazlullah Khan, Fahim Arif, Qamar Jabeen, M.A Jan and S. A Khan (2016). "Performance Improvement in Wireless Sensor and Actor Networks", Journal of Applied Environmental and Biological Sciences, Vol. 6(4S), pp. 191-200, Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[36]. M. Usman, M. A. Jan, X. He and P. Nanda, "Data Sharing in Secure Multimedia Wireless Sensor Networks," *in 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16)*, "accepted", 2016.