International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 158-162, 2018, ISSN:-2319–8656

Addressing Security Issues and Challenges in Mobile Cloud Computing

Nirmal Kumar Gupta
Jaypee University Anoopshahr
Anoopshahr, India

Gaurav Raj
Jaypee University Anoopshahr
Anoopshahr, India

Abstract: The emergence of cloud computing has brought tremendous impact on software organizations and software architecture design. With the development of cloud computing and mobile internet, mobile cloud computing is becoming a new mode of application. With the widespread development of mobile applications and advances in mobile cloud computing, some other forms of requirements and security issues have been emerged. Mobile cloud computing provides resources residing over cloud and services provided for mobile devices. These resources and services from cloud are available for mobile user over their mobile devices. It also provides benefits for developing specialized mobile applications for them. However, increased security and privacy risks exists due to data outsourcing and synchronization over the Internet. This research paper provides the review on mobile cloud computing, its security issues, challenges and suggests some solutions.

Keywords: mobile cloud computing, cloud security, privacy, data security, challenges

1. INTRODUCTION

In today's world of computing, cloud computing has provided a new kind of computing environment different from traditional computing, in which hardware, software and other services are provided on-demand in a virtualized manner. Cloud computing provides a service model which uses the network to access shared resources to access remotely hosted computing resources to the clients for their business needs.

The basic service model of cloud computing utilizes Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Services (IaaS) for providing various services [1]. Mobile Cloud Computing (MCC) is a computing idea which connects mobile computing with cloud computing. MCC combines the benefits of mobile computing and Internet used on mobile devices with cloud computing [2]. That is the reason for MCC to be called as cloud computing services using the mobile Internet. MCC has enabled the data storage and its processing possible outside the mobile device. Instead of storing the software and data over the Internet rather than on a single device, cloud computing seems to provide on-demand access to resources and services. Using MCC the earlier intensive computations performed on mobile devices, storage of data and other control information has been transferred to the cloud and therefore the computing power and resources available with mobile devices are left to be used for some other useful work. It also has facilitated for mobile cloud applications and data storage to be shifted from mobile phones to the cloud, thus enabling the applications and mobile computing to reach a broader range of mobile users, not just smartphone users.

2. MOBILE CLOUD COMPUTING ARCHITECTURE

In MCC, the mobile network and cloud computing are combined to provide the best service to the mobile users. Since data and software is stored over the Internet instead of on a single device, cloud computing is able to provide on-demand access. The application runs on the remote server and sends the results to the user. The overview of mobile cloud computing architecture is shown in Fig. 1. In this architecture, the individual mobile device is connected to the base station of the mobile radio network. There exist Base Transceiver Stations (BTS) which facilitates mobile devices to communicate with the network. Their purpose is to provide an interface to establish a network connection between mobile devices and the network. The requests generated from the users are communicated over the wireless network to the cloud through the mechanism called Authentication, Authorization and Accounting (AAA). Once the requests generated from the users is reached to the cloud, these requests are processed through the cloud controller and corresponding cloud service accesses these requests.

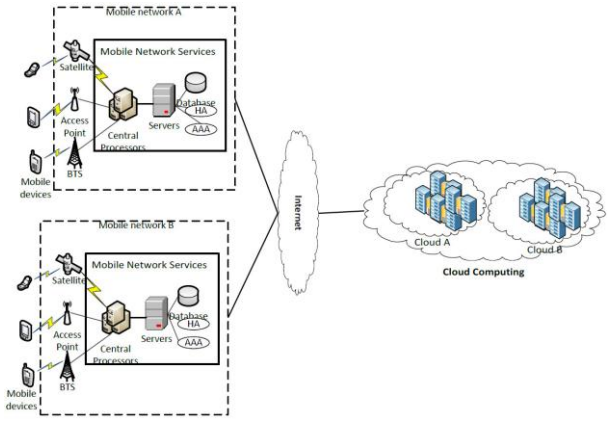


Fig. 1. Mobile Cloud Computing Architecture [3]

3. CHARACTERISTICS OF MOBILE CLOUD COMPUTING

Mobile Cloud Computing has some major characteristics which includes Security, Reliability, Scalability, less maintenance, less cost and platform independence etc. [4]

3.1 Computing as a Service

A very fundamental principle of cloud computing is that it is considered "as a service" where specific services are provided through cloud to its users by the cloud service provider. The services provided in this way are generally categorized based

upon the applications used through it [5]. Here are some examples of areas of application offering services: like financial, managerial or analytical. For using the services through the cloud there must be some agreed terms of use between user and service provider. Such an agreement describes the actions which can be taken in case of failure from either side. This failure can result in denial of service to the customer from the service provider or may result in a legal liability for service provider. Besides the actions which could be taken from either side, such agreement also includes a privacy policy which describes the way in which a user's data will be stored and managed for its privacy.

3.2 Service Model

The services provided by cloud computing are generally classified using SPI (SaaS, PaaS, IaaS) model which represents the various levels of services provided by the service provider to the user through the cloud services. Using SPI model the various services such as the software to be used for development of some application, the platform required or other needed infrastructure can be provided in a seamless manner [6]. SPI service model is summarized in Fig. 2.

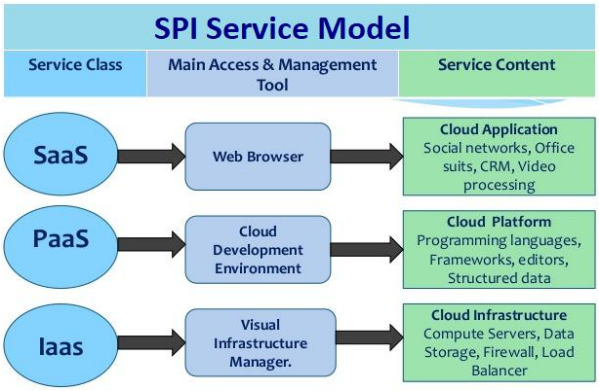


Fig. 2. Summary of the SPI Service Model

3.2.1 Software as a Service

The highest layer of SPI model is "Software as a Service" (SaaS). The applications needed by the users are hosted through SaaS layer of SPI model which provides protocols and other services through the network, defined by the service provider. With the development of support technologies for a better web services the use of SaaS is becoming more popular. Once the service provider is chosen carefully security of data can be assured.

3.2.2 Platform as a Service

The PaaS provides the next layer of SPI model which is mostly used as a software development platform by the software developers. This layer provides the services which are used by the developers to write code and manage it through the use of the cloud. In this regard cloud is used to provide development tools and data management and other services required for security.

3.2.3 Infrastructure as a Service

The last and lowest level of SPI model is known as Infrastructure as a Service (IaaS). IaaS is a single-tenant cloud layer where the provider of cloud services provides dedicated resources, which are shared among different customers. Therefore, the requirement of for a large starting investment of various hardware resources including networking devices, servers, switches etc. are minimized. Such provisions provide a greater degree of flexibility in terms of achieved functionality and economically. Such kind of flexibility are generally not available in centralized data and hardware centers. Whenever needed more resources can be added in less time over cloud which can be utilized by the users.

4. SECURITY IN THE MOBILE CLOUD COMPUTING

One of the major issues about MCC is that most cloud providers are concerned about is ensuring the privacy of the user and the integrity of data or applications. Security issues in MCC must be handled in an effective manner because it considered is a combination of mobile networks and cloud computing. We can divide security issues mainly in two categories:

1. Security issues associated with the cloud
2. Mobile network user's security

4.1 Security issues associated with the cloud

The various technologies like virtualization, operating systems, scheduling of resources, database management, concurrency control, load balancing and memory management etc. are included in cloud technologies. This introduces various security related risks in cloud whose intensity and nature may be different than the risks associated with traditional software and services [7]. Figure 3 shows data protection risks to regulated data [8] Network connection dependency and data sharing. Integrating applications and security are some of the major challenges in MCC environment.

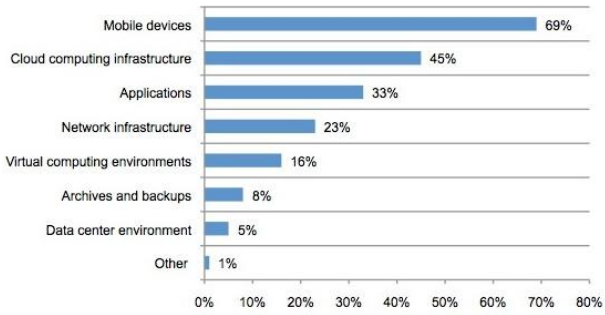


Fig. 3. Data Protection risks in MCC

In MCC, sharing of infrastructure between multiple clients may cause the risk of data visibility by other users. In addition, cloud users want to ensure that critical data is not accessible and utilized illegally, even by cloud providers. Since the web-based interface is used for on-demand services to be provided to clients which causes the probability of unauthorized access to the interface which might be higher than the traditional systems. According to Gartner [9], before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. According to [10], there can be two types of communication, namely, external "customer-to-cloud" communication and internal "cloud-to-cloud" communication. In the first case the cloud services are accessible via the internet using standard internet mechanisms and protocols to transmit data or applications between clients and the cloud. This type of communication is similar to any other communication on the Internet. Indeed, data in transit can be the target of several malicious attacks [9] [10]. These attacks include denial of service (DoS), eavesdropping, identity theft, altered

environment etc. The second type is related to the communication between the VMs. This communication is targeted for malicious attacks because of the various factors which includes the shared communication infrastructure, the virtual network, and the bad security configuration. Cloud security has close relationship with the corporate security policies. They must go beyond the difficult requirement of passwords and login privileges. It is necessary to move to the next level and think about security in terms of usage and types of data. The more sensitive they are, the higher the security must be and the more the choice of the type of Cloud is critical and crucial.

The level of security of the public cloud is not optimized for professional use, but its flexibility and value can make it attractive to many small organizations. The Private Cloud is based on the same principle as the public cloud, but it is of course owned by a company and intended for a smaller number of users, customers or partners of the company owner. Finally, the hybrid cloud is a mix of private and public clouds. It is made up of several internal and external partners. Its interest lies in its ability to navigate data between the public and private according to their sensitivity to optimize costs. Regardless of its type, cloud solution providers rely on a mix of proprietary and open source code to ensure the security and integrity of the data they host and protect. According to [11], whatever the form of the Cloud Computing contract is, this contract must absolutely include these five key points, namely, data localization, law and Jurisdiction, service levels provided by the MCC provider, reversibility and access to data and data security. In addition, the order of importance of these five key points will vary according to the service used (IaaS, PaaS, SaaS) and its purpose (storage space, development environment, billing tool).

According to [12], cloud security challenges are the dispersion of international data and privacy laws, the need to be addressed for various issues like local management, multi-tenancy, logging challenges, data ownership issues, and Guaranteed quality of service, dependence of secure H-viewers, interest for hackers, security of virtual OS in the Cloud, possibility of massive interruptions of service, encryption needs for security in the Cloud, public cloud security versus private cloud security etc. According to [13], there are nine main risks, namely Data Breaches, Data Loss, Account Hijacking, Insecure APIs, Denial of Service, Malicious Insiders, Abuse of Cloud Services, Insufficient Due Diligence and Shared Technology Issues. Regarding the legal responsibilities for data security and privacy in the cloud, according to [13], they find that the customer is legally responsible for its data and usage, including anything concerning their compliance with legal obligations, while, the provider is subject to technical and organizational obligations. It is committed to preserving data integrity and confidentiality, protecting and recovering data, encrypting data etc.

4.2 Mobile network user's security

Some of the security concerns in mobile network user are discussed below:

Loss of control over data: The paradigm of MCC is changing the way information is managed, especially with respect to the processing of personal data. Storing personal data on a server somewhere in cyberspace could pose a great threat to privacy. Because tenants and users lose physical control over their data and applications, this raises a number of issues.

Data security and privacy: With public or community clouds, the data may not remain in the same system, which poses multiple legal problems. The biggest concern that everyone seems to agree with the cloud is security. Data security and privacy are at the forefront of almost all the concerns. The main challenge for MCC is how it addresses the security and privacy concerns of the companies that are considering adopting it [14]. The fact that the company's valuable data resides outside the company's firewall raises serious concerns. Piracy and various attacks on the cloud infrastructure would affect multiple clients, even if only one site is attacked. These risks can be mitigated through the use of security applications, encrypted file systems, data loss software and purchase of security hardware to track unusual server behavior.

Data control: Data can reach the provider in several ways with some data belonging to others. A host administrator has a limited scope of control and accountability within a public infrastructure implementation as a service (IaaS), not to mention a platform as a service (PaaS). Hosts must have confidence that their provider will provide adequate control, while recognizing the need to tailor their expectations to the amount of reasonable control in these models.

Quality of service: quality of service is one of the most important factors that companies consider a reason not to move their commercial applications to the cloud. They consider that SLAs (Service Level Agreements) provided by cloud providers are not currently sufficient to guarantee the requirements to run cloud-based development applications, particularly in terms of availability, performance, reliability and scalability. In most cases, companies are reimbursed for the duration of the non-availability of the service, thus most current SLAs reduce commercial losses [15]. Without a guarantee of service quality, companies will not host their critical infrastructure in the cloud.

Transparency: When a cloud provider does not expose the details of its own internal policy or technology, hosts or users must rely on vendor security claims. Hosts and users may still require some transparency from providers as to how they handle security, privacy, and security incidents in the cloud.

Legal and Regulatory Compliance: It may be difficult or unrealistic to use public clouds if your data is subject to legal restrictions or regulatory compliance. You can expect vendors to create and certify cloud infrastructures to meet the needs of regulated markets. Achieving certification can be a challenge because of the many non-technical factors, including the current state of general knowledge of the cloud. As best practices for MCC encompass a broader scope, this concern should disappear.

Incompatibility Issue: The storage services provided by a cloud service provider may be incompatible with the services of another provider in case some user decides to switch from one to the other. Providers are known for creating what the world of hosting calls "persistent services," services that an end user may have difficulty moving from one cloud provider to another.

Performance and cost of bandwidth: Companies can save money on hardware, but they have to spend more on bandwidth. This can be a low cost for a smaller application, but it can be high for an application that requires a large amount of data. Providing intensive and complex data through the network requires sufficient bandwidth. For this reason,

many companies expect a reduced cost before moving to the cloud.

Low Performance of the network: the provision of complex services through the network is clearly impossible if the bandwidth of the network is not enough. Many companies expect improved bandwidth and lower costs before considering switching to the cloud. Many applications in the cloud still consume too much bandwidth.

Integration: Many applications have complex integration needs to connect to other applications in the cloud, as well as other local applications. This includes the integration of existing cloud applications with enterprise applications and existing data structures. It is necessary to connect the application in the cloud to the rest of the company in a simple, fast and profitable way.

5. SOME SOLUTIONS TO SECURITY PROBLEMS IN MCC

The correct implementation of security measures is mandatory in MCC to provide a secure infrastructure that can only ensure and increase confidence that the stored data is safe with the service provider. This can be achieved by the following means:

Data encryption: In the public cloud, resources are shared by multiple users in the cloud and, as a result, the responsibility of their providers is to entrust the separation of data to their customers. Data encryption is a common approach that providers follow to protect their customers' data, but the question is whether the data is stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store critical data, organizations can think of a private or hybrid cloud where the data will be in a secure corporate firewall. An important way to increase data protection, privacy and integrity is to ensure that data is protected in transit and when stored in the cloud by using file-level encryption. As CSA (Cloud Security Alliance) [16] Guidance notes, “Encryption offers the benefits of minimal use of the cloud service provider and dependence on operational failure detection.” Encrypted data-centric protection means that data cannot be used by anyone without the key to decrypt it. It does not matter if the data transmits or is stored, it remains protected. The owner of the decryption keys maintains the security of this data and can decide whom to allow access to what data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an administrator could encrypt all data in the backup before sending them to the storage cloud. One of the best security solutions for cloud and virtualized environments is portable encryption at the file level, focused on data on all computer platforms and operating systems, and operates in a private, community, public or hybrid cloud.

Refactoring Data: Simply applying the encryption method does not guarantee the security of the data transfer. In the case of data transmission, the greatest risk is related to the encryption technology in use. Instead of using encryption and decryption, the data can be divided into smaller packets that can then be transmitted to the receiver through different routes. Such an approach will reduce the chances of capturing information by unauthorized persons. The data does not make sense unless all the data is received.

Restricted access: Restricted user access can range from simple username/password protection to some challenge-response test in login forms. When an employee no longer needs to access the data center, their access privileges to the data center must be immediately revoked. Cloud providers can also consider password authentication at a time when customers will get a temporary password from the SSN/mobile device, which contributes to data security even if the password is compromised.

Backup and recovery: In MCC, the data is stored in a distributed location. Cloud clients will never be able to determine the exact storage location of their records and the importance of data backup and recovery appears. The backup software must include cloud-based APIs, which allows simple backup and recovery in the main cloud storage providers. The backup and restoration services guarantee that one can always recover the data. A questionable question is whether to back up all the data or make a backup of critical and vital data. If the provider agrees to save crucial data, the question is how to determine the priority of the data. The simplest and least complicated way is to protect the entire workstation or server. It is essential that the backup application encrypts confidential data before sending it to the cloud off-site, protecting data in transit through a WAN to a storage location in the cloud and data storage on the site as cloud storage.

Access control: Access control and management of user profiles become more complex with cloud services because information sources can be hosted somewhere other than the cloud service that needs them. Clients must identify reliable sources for this information and ensure mechanisms to transmit information from the reliable source to the cloud service. It is also important to periodically reconcile the information between the cloud service and the source. Customers must confirm that cloud providers support their access control requirements appropriately for cloud resources.

6. CONCLUSION

Mobile Cloud Computing (MCC) is an emerging and futuristic technology due to the variety of benefits and applications offered to mobile subscribers. The main reason for the possible success of MCC and the great interest of organizations around the world are due to broad category of services provided with the cloud, but the current technology does not provide all the requirements that MCC needs. Researchers face many challenges to make MCC work in reality. Besides the various benefits provided through MCC some security issues need to be addressed to ensure that it is a safe and reliable services could be provided. This paper has discussed some security issues and possible solutions concerning MCC. Securing MCC user’s privacy and integrity of data or applications is one of the major issues most cloud service providers have given attention.

7. REFERENCES

1. Luo, J.Z., Jin, J.H., Song, A.B. and Dong, F., 2011. Cloud computing: architecture and key technologies. Journal of China Institute of Communications, 32(7), pp.3-21.

2. Dinh, H.T., Lee, C., Niyato, D. and Wang, P., 2013. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), pp.1587-1611.

3. Prasad, M.R., Gyani, J. and Murti, P.R.K., 2012. Mobile cloud computing: Implications and challenges. Journal of Information Engineering and Applications, 2(7), pp.7-15.

4. Padma, M. and Neelima, M.L., 2014. Mobile Cloud Computing: Issues from a Security Perspective. International Journal of Computer Science and Mobile Computing, 3(5), pp.972-977.

5. Krutz, R.L. and Vines, R.D., 2010. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.

6. Mell, P. and Grance, T., 2009. Effectively and securely using the cloud computing paradigm. NIST, Information Technology Laboratory, 2(8), pp.304-311.

7. Ali, M., Khan, S.U. and Vasilakos, A.V., 2015. Security in cloud computing: Opportunities and challenges. Information Sciences, 305, pp.357-383.

8. Donald, A.C., Oli, S.A. and Arockiam, L., 2013. Mobile cloud security issues and challenges: A perspective. International Journal of Electronics and Information Technology (IJEIT), ISSN, pp.2277-3754.

9. Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02.

http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.

10. Chen, S., Nepal, S. and Liu, R., 2011, September. Secure connectivity for intra-cloud and inter-cloud communication. In Parallel Processing Workshops (ICPPW), 2011 40th International Conference on (pp. 154-159). IEEE.

11. Rohrmann, C.A., Cunha, S.R. and Falci, J., 2015. Some legal aspects of cloud computing contracts. J. Int't Com. L. & Tech., 10, p.37.

12. Kshetri, N., 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4), pp.372-386.

13. Los, R., Shackleford, D. and Sullivan, B., 2013. The notorious nine cloud computing top threats in 2013. Cloud Security Alliance.

14. Bhadauria, R. and Sanyal, S., 2012. Survey on security issues in cloud computing and associated mitigation techniques. arXiv preprint arXiv:1204.0764.

15. Das, S., Kagan, M. and Crupnicoff, D., 2010. Faster and efficient VM migrations for improving SLA and ROI in cloud infrastructures. DC CAVES.

16. Everett, C., 2009. Cloud computing–A question of trust. Computer Fraud & Security, 2009(6), pp.5-7.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 163-170, 2018, ISSN:-2319–8656

Building Blocks for Eco-efficient Cloud Computing for Higher Learning Institutions in Tanzania

Rodrick Frank Mero
Department Information Communication Science and Engineering
NM-AIST
Arusha , Tanzania

Abstract: Owning and managing a cloud-computing infrastructure, i.e. private data centers (DC), is a feasible way forward for an organization to ensure security of data when opting for cloud computing services. However, the cost associated with operating and managing a DC is a challenge because of the huge amount of power consumed and the carbon dioxide added to the environment. In particular, Higher Learning Institutions in Tanzania (HLIT) are among the institutions which need efficient computing infrastructure. This paper proposes eco-efficient cloud computing building blocks that ensure environment protection and optimal operational costs of a cloud computing framework that suffices HLIT computing needs. The proposed building blocks are in a form of power usage (renewable and nonrenewable); cloud deployment model and data center location; ambient climatic conditions and data center cooling; network coverage; quality of service and HLIT cloud software. The blocks are identified by considering HLIT computing requirements and challenges that exist in managing and operating cloud data centers. Moreover, this work identifies the challenges associated with optimization of resource usage in the proposed approach; and suggests related solutions as future work.

Keywords:Cloud computing, Building Blocks, Higher Learning Institution in Tanzania, Power consumption, eco-efficient, Traditional computing , Data Center

1. INTRODUCTION

Cloud computing has been trusted as a technology of choice in most resource provisioned in academic environments [1, 2, 3]. Despite the flexibility and cost effective services offered by cloud computing, none of the Higher Learning Institutions in Tanzania (HLIT) has jumped onto the bandwagon. These institutions still use traditional computing (TC) that has been proven to be uneconomical in terms of maintenance and software purchase costs [4]. Moreover, the shortage of stable power supply prevalent in the country and lack of ample funding faced by most HLIT necessitate the development of computing solutions which are eco-efficient.

In order to develop an eco-efficient cloud computing framework that suits an academic environment, there is a need for addressing existing computing challenges [5, 6]. These include high operational costs and carbon dioxide emissions by cloud data centers, and poor guarantee in quality of service (QoS) as per Service Level Agreements (SLA). Therefore, the building blocks of the framework should be able to address these challenges.

In general, building blocks are all requirements such as: technology, policies, cloud best practices, software and infrastructure that support in building and adoption of economical, efficient and environment friendly cloud computing solutions. Normally, cloud architecture is made of layers; each layer is designed to provide a service such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [7]. Thus, eco-efficient building blocks should also be able to address the complexity of each layer according to the underlying cloud computing architecture.

Principles for eco-efficient building block selection.

Design principles that guide selection of specific eco-efficient building blocks are characterized by features which consider the economical, technological and environmental challenges that exist in the designated environment for cloud computing services. The criteria for eco-efficient building blocks selection are as follows:

a) HLIT as other academic institutions in the world are in need of cost effective solution to their existing computing challenges, therefore, focusing on free and open source software (FOSS) is an important criterion in selecting cloud software. Likewise, choosing cloud deployment model should consider its operation costs and challenges relative to a Traditional Computing (TC) system.
b) Huge power consumption and environmental pollution by current cloud data centers have been a challenge to data center operators; thus focusing on green aware and low power consumption technologies is an important criterion.
c) Efficiency and flexibility of computing solution are very important for its acceptance; thus cloud computing building blocks should guarantee quality of service. Accordingly, network connections must ensure reliability and availability of cloud computing services to end users. Moreover, virtual machine consolidation should not impact performance of cloud services.

To this end, this work has identified building blocks needed for developing eco-efficient cloud computing that aligns with the guidelines and issues related to green power utilization.

The remaining sections of this work are organized as follows: Section 2 presents eco-efficient building blocks that are necessary to align with eco-efficient cloud requirements for HLIT, Section 3 presents related works and Section 4 concludes and discusses the work while suggesting future directions.

2. Eco-efficient Building Blocks

As mentioned in previous section eco-efficient cloud computing building blocks refer to all requirements such as technology, policies, cloud best practices, software and infrastructure that support building and adoption of economical, efficient and

environment friendly cloud computing. In this chapter, we focus on environmental, technological and infrastructure building blocks.

Generally, cloud computing is made up of data centers that are connected using high speed network connections [8]. Each data center is made up of a large number of hosts, in each host there are virtual machines (VMs) that act as user PCs. VMs run as normal processes in computing systems. What distinguishes VMs from normal process is their capability to virtually work like physical hardware with operating system (OS), memory, processor, and storage. Thus, the act of purchasing a new PC in a TC scenario can be replaced by a request for a new virtual machine in the cloud.

To ensure efficient and green aware computing in HLIT, an eco-aware cloud framework is inevitable. Development of such a green cloud needs clear identification of well suited technological building blocks (i.e., networks, efficient cooling infrastructure, operating system (OS), cloud management tools) in all layers of the cloud architecture (i.e., IaaS, PaaS, SaaS). As academic eco-efficient cloud-computing services expect to be accessed by a large number of users, especially students and researchers, efficiency and scalability of cloud resources in such multiuser and dynamic environment have to be guaranteed.

For efficient cloud operation and coordination of data center resources, we identify and propose the building blocks that suffice HLIT cloud computing needs, see Fig 1. The building blocks are in the form of nature of power source (i.e., renewable and nonrenewable); deployment model and data center location; ambient climatic conditions and data center cooling; network coverage; quality of service and HLIT cloud software.

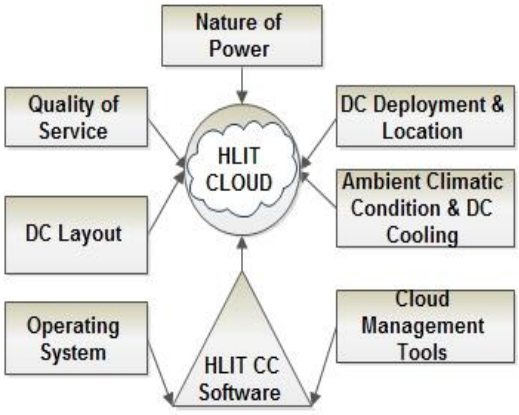


Fig 1 Building Blocks

2.1 Form / nature of Power

Tanzania like other developing countries has a low level of electrification [9] while the need for electric power consumption is increasing year after year [10, 11]. As cloud data center power consumption could be similar to that needed to power a city, the need to consider energy efficiency becomes very important. Otherwise, providers would incur huge operational costs to maintain data centers (Markoff & Lohr, 2009). Therefore, consideration of renewable energy sources becomes very important in avoiding a huge amount of carbon emission from bio-fuels.

Today's data centers are powered by different sources of energy. Data centers draw power from local electric grids. These grids are powered by either fossil-fuel based brown energy, renewable resource based on green energy or more commonly a combination of both. Hydro power plants are among few electric power production centers in Tanzania. Hydro production centers are located at Nyumba ya Mungu, Kidatu, and Mtera. Other sources of electrical power that are connected into the national grid are from fossil-fuel sources (petroleum, diesel); for example, power generated by Songas Company from Ubungo, Tegeta and other locations. It is difficult to distinguish power from renewable sources and fossil-fuel in the national grid [8] Although to locate a data center near Kidatu or Nyumba ya Mungu regions will result in more usage of renewable energy than placing them close to fossil fuel power sources [12]. Similarly, processing user request by considering closest path can bring challenges because a large number of users' requests can overload a single data center. Comparing data-centers located closer to renewable power production sites (i.e. Kidatu, Mtera) with ones located close to nonrenewable power production sites (i.e. Tegeta and Ubungo); access frequency of virtual machines located in Ubungo is considered to be higher due to expected large number of requests from HLIT closer to that area.

Therefore, challenges are in terms of optimization of workload, power consumption and carbon dioxide emission. Moreover, temperature and drought seasons bring challenges to hydro power generation.

The proposed approach in this chapter is to utilize both renewable and nonrenewable power sources appropriately. In the same vein, developing a Heuristic that can minimize tradeoff between power consumption, quality of service and carbon emission in such environment is an important concern. For example, migrating VMs from over-provisioned hosts in Ubungo data center to under provisioned data center in Kidatu or Nyumbaya Mungu should result into reduction of considerable amount of carbon emission; but leads to tradeoff between green aware consolidation and migration costs.

2.2 Cloud Deployment model and data center location

As discussed in [4], the Hybrid model is the preferred deployment model for HLIT. This model is suitable for academic environment because it combines advantages that exist in public and private cloud [13]. Hybrid model maintains private data center that can support complex mixed workloads. This model makes utilization of local IT infrastructure as private cloud with other selected service from public. As observed in [4], HLIs are facing challenges such as lack of constant power supply, inefficient cooling systems, and redundant of inefficient IT infrastructure. These issues raise concerns on capability for an institution to own and manage a private data center. The cost effective and reliable way is to locate a private data-center in a zone where it can be accessed by HLIs with optimal access costs. This strategy minimizes data center operational costs that could be incurred by a single institution.

Geographical location of a data center plays an important role. A data center located in an area with easy access to hydro power, for example, would have a lower carbon footprint than a data center located in an area that depends on coal, oil, or natural gas [14]. In the HLIT hybrid cloud model, private data center should be positioned by considering factors such as availability of renewable energy resources, availability of enough bandwidth, i.e. accessibility to the National ICT Broadband Backbone (NICTBB). It is important to locate a data center in a region where temperature is very low in order to reduce the need of having large

number of cooling systems that can increase data center energy consumption. A geographical location that experiences high temperature and humidity levels will consume more energy as the data center physical infrastructure systems work harder to maintain consistent, moderate temperature and humidity levels [14]. Seemingly, locating data center close to renewable resources will make utilization of energy/ power from green energy sources that results in reduction of carbon footprint into the environment. From this point of view, data center location, IT load, and electrical efficiency are important factors to be considered when building and managing a data center.

2.3 Ambient climatic conditions and data center cooling.

The Green Grid [15] outlined seven strategies to improve data center efficiency. One of the proposed practices which can lead to improved power consumption is the use of free cooling. The American Society for Heating Refrigeration and Air conditioning Engineers (ASHRAE) defined operating range that different types of data centers can operate. The range specifies how climatic condition can affect data center cooling. To exploit advantage of data center free cooling temperature characteristics of data center expected location should be monitored. For a case of HLIT climatic condition of each zone is as indicated in Table 1.

Table 1 Tanzania average regional Temperature. [Source: TMA1]

	Zone Name	AVR Min Temp	AVR Max Temp
1	Western	16	25
2	Eastern	25	33
3	Southern	17	27
4	Northern	20	27
5	Central	18	27

In order to have eco-aware data centers; the use of the nature of climatic conditions in identifying a possible cooling framework should be in accordance to the [16, 17] guidelines. The free cooling strategy has been used to lower Power Unity Effectiveness (PUE) of data centers. Free cooling involves the ability to use local ambient conditions to remove heat from inside a data center [18, 17]. To relate cooling and PUE we have,

$$PUE = \frac{TFE}{ITE}, \qquad (1)$$

where TFE is total facility energy, and ITE is IT energy. TFE includes power that is used by data center supporting infrastructure such as cooling system and Uninterrupted Power Supply (UPS). Use of air conditioners and electrical fans raises TFE. Free cooling lowers PUE by minimizing TFE through the use of climatic ambient conditions.

There are two forms of free cooling techniques, air-side and water-side cooling. Air-side cooling uses air economizer to bring the coldness of outside air into the data center to cool servers below the specification indicated in ASHRAE'S thermal guidelines (The 42u.com, 2014). Water-side economizers use cold air to cool an exterior water tower. Water side economizer gives good result for the climatic condition where temperature is below 12.78 degree centigrade for 3000 hours or more [19]. In HLIT environment, the average temperature range is above specified requirement, thus we won't consider water economizer in our work. The next part analyzes the use of air-side economizer as a cooling strategy for private data centers in HLIT clouds.

Air-side economizer pumps fresh air into a data center and hot air is exhausted. A system that can deliver 3m3 of air can consume 1.5 kW, and save up to 30kW [20]. For the climatic conditions described in [21], relying on air economizer in 91% of the year can save approximately 67% of the total power used annually for cooling compared with a traditional data center cooling approaches. Temperature characteristics of possible data center location as seen in Table 1 prove the feasibility of using air-side economizers. The minimum temperature in all zones is within ASHRAE recommended range. Similarly, the maximum temperature of zones except eastern is below maximum ASHRAE recommended range. For full use of economizer, one host may reallocate its workload to another host in a location where the use of an air-side economizer is feasible. During the night, temperature is considerably low, (minimum zone temperature in Table 1) therefore, air-side economizers can be used in all zones.

2.4 Data Center Layout for Free Cooling

One major data center design principle is efficient air flow management within a data center that can be achieved by optimal positioning of data center equipment [22]. Air flow management entails all the design and configuration details that go into minimizing or eliminating a mixture between the cooling air supplied to equipment and the hot air rejected from the equipment. To achieve economical cooling circulation of air, the cooling system should be able to remove hot exhaust air before exhausting, and the heat it carries is mixed with cool fresh air. To make sure that drawing and exhaust airs are not mixed, data center equipment is laid out in rows of racks with alternating cold (rack air intake side) and hot (rack air heat exhaust side) aisles between them; as shown in Fig 2.

[1]Tanzania Meteorological Agency (2014)

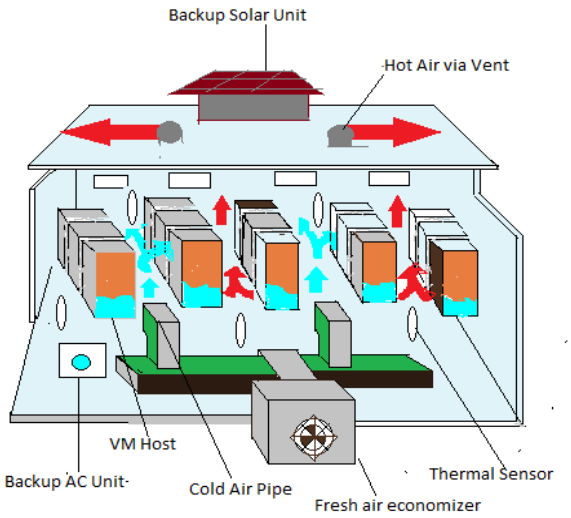


Fig 2 Efficient cooling model for data center

Air-side economizer draws outside air and distributes between and above the racks. Exhausted hot air is pushed out of the racks via a vent. To ensure service availability safety of data center during climatic variations, backup AC unit can be incorporated. AC should be powered using renewable power sources to avoid addition of carbon foot print during its operation. Distance between server and racks, racks and racks, server and server should be enough for smooth maintenance and server configuration. Air-side economizer distribution unity can be overhead or underfloor depending on the type of the rack used to allow effective cooling.

2.5 Network Coverage

VM migration requires a high-bandwidth connection from user to destination data centers [8]. In order to maximize data center efficiency, a cloud user request should be processed in the data center that have optimum resource cost while ensuring minimum migration overhead. Let α describe the cost associated with single VM migration across a network, then:

$$\alpha = < V, Ns, Nd, B, D, T > \quad (2)$$

where, V is the VM to be migrated to, Ns is the source location, Nd is the destination location, B is the required connection bandwidth, D is the connection holding duration, and T is the time when the migration shall start. Thus, the total data volume to be transferred if the request is satisfied is given by B × D [8].

Any placement of a VM to a host should minimize migration cost while taking care of performance and quality of services (QoS). For the case of HLIT, it was found that cloud bandwidth requirements in all zones can be achieved based on accessibility of the NICTBB. In addition, the nature of power sources that are available supports the use of renewable energy sources to power cloud data centers. Having network infrastructure support, enriches zoning data center placement strategy that makes efficient use of available resources by allowing flexibility in consolidation of VMs from one zone to another when cloud services are not meeting desired requirements.

2.6 Quality of Service

While optimal location of data center, network coverage and nature of power source are important data center building blocks, quality of service during data center operation should be achieved. Virtualization of computing services should not impact performance that a user experiences on using non virtualized services. The percentage by which virtual machine consolidation is violating the SLA should be considered while minimizing cloud data center energy usage and carbon emission. Usually, QoS can be degraded by the following factors: (1) the fraction of time during which active hosts have experienced CPU utilization of 100%, i.e., Overload Time Fraction (OTF); and (2) the overall performance degradation by VMs due to migration, i.e., Performance Degradation due to Migrations (PDM) [23]. OTF and PDM metrics should be optimized by having an efficient resource allocation strategy.

2.7 HLIT Cloud Software (OS, management tool, hypervisor)

When deciding the best possible design for building HLIT hybrid cloud, we came across a wide range of cloud management and monitoring tools, and operating systems for which to install these components. Due to the heterogeneity of cloud computing, it is important to choose a suitable tools platform to manage virtual machines and hosts. In this study, various tools were identified. Their analysis led to the selection of those in favor of our design environment and objective.

2.7.1 Operating System

One of the most important ways to support the underlying complexity of well-managed cloud computing resources is through the operating system (OS) [24]. Operating system such as Debian, Openness, Ubuntu Server, Linux and others are created to support these requirements so that cloud and application services should not recreate underlined technologies tailored to each deployment. The best OS support balanced workloads and can scale in a secure manner.

Debian is a free and open source operating system which includes GNU operating system tools and a Linux kernel. It is compatible with Xen and has a GUI integrated with it. Openness is also a free and open source operating system made up of a series of software packages. It includes GNU operating system tools and a Linux kernel. It is compatible with Xen and includes both a default Graphical User Interface (GUI) and a command line interface option. Ubuntu Server Edition also runs on VMware ESX Server, Oracle's VirtualBox and VM, Citrix Systems XenServer hypervisors, Microsoft Hyper-V as well as Kernel-based Virtual Machine [25]. Ubuntu server supports a major two architectures; Intel x86 and AMD64. The server edition uses a screen mode character-based interface for the installation instead of a graphical installation process. It consists of open core Eucalyptus, libvirt, and KVM or Xen virtualization technology.

Reilly and Cearra, (2012) investigated different operating systems in order to test which one is suitable for hybrid cloud infrastructure. From the experiment, Ubuntu Server was found to be the most efficient operating system under a hybrid cloud environment. As a point to remember, Ubuntu server is a FOSS. It is furthermore compatible with other cloud software's such as Xen, Open Nebula, CloudStack and others. This makes a strong point to propose Ubuntu server to be an operating system to run on servers for hybrid cloud computing for HLIT.

2.7.2 Cloud management tool (CloudStack)

Building a data center in a distributed environment raises the need of software which can manage the complexities and the heterogeneity of cloud workload in a mixed demand environment.

The candidate that can fit in that environment is an Open-source software called CloudStack. CloudStack is a software platform that pools computing resources to build public, private and hybrid IaaS clouds [26]. CloudStack gives a cloud developer the ability to extend the cloud resources allocation policy through the use of pluggable allocation architecture that allows the creation of new types of allocation policy. It supports zoning architecture which is the desirable model for HLIT. It divides cloud infrastructure into Zone, Pod, Cluster and final host. Its nested architecture gives high flexibility in managing and configuring cloud resources. In addition, CloudStack is built with a number of VM monitors, and network configuration features that are flexible to multiple design environments.

2.8 Data center distribution architecture

Fig 3 shows the proposed data center distribution in different zones of the country. Each data center placement is influenced by accessibility to NICTBB and availability of renewable power resources and ambient climatic conditions that allow free cooling.

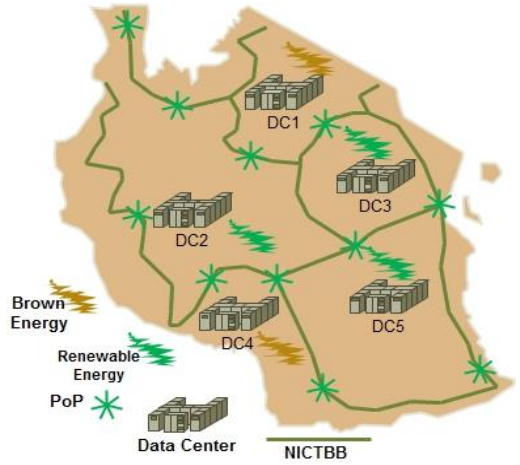


Fig 3 HLIT Cloud Computing Data centers distribution

3. Related works

Several cloud academic computing frameworks have been proposed [13, 27, 1]. With similar concerns of establishing efficient computing systems for academic services; Saidhbi (2012) proposed alternative solutions to solve the current IT utilization, and limitations in Ethiopian Higher Education Institutions. The author proposed hybrid cloud framework to enhance academic requirements. The proposed framework combines multiple services from different cloud service providers (CSPs) to serve students and other users from different universities to enhance the teaching, learning and service delivery. OpenNebula is the proposed cloud management tool; on top of OpenNebula, Aneka middleware layer is added to manage PaaS. The framework is designed to utilize power aware techniques that are in OpenNebula. Suryawanshi and Narkehde, (2012) proposed the cloud framework for higher technical education. The framework includes three deployment models (i.e. private, public and hybrid). The framework is structured into four layers SaaS, PaaS, IaaS and hardware. SaaS layer is divided into four components which are faculty, student, staff and research. The suggested framework does not address today's data center power consumption problems. However, Beloglazov et al, (2012) and Esfandiarpoor et al (2013) recommended power aware data center heuristics that reduce carbon dioxide and power consumption. In the work, performance and QoS of a data center were analyzed. Virtual machine consolidation heuristics were developed. The heuristics lower power consumption of host by shutting down underutilized and idle servers.

Choosing cloud solution according to its usage environment is very important on selecting cloud building blocks. Singh and Hemalatha, (2012) suggested academic cloud that suits storage infrastructure, development platform, and software delivering environment. The proposed framework separates user data on cloud by providing user with a password secured virtual storage. The framework was enriched with high performance features in order to outperform thin client computing system being used in academic environment. Open source solution has been used by Pantić and Babar, (2012) to develop private cloud infrastructure that suits organizational environment. Building blocks of the proposed private data center were made up with Ubuntu Enterprise Cloud (UEC), which is a combination of Ubuntu Server Edition with Eucalyptus. Bundling blocks make UEC easier to install and configure the cloud. On the other hand, it uses the same API's as Amazon making hybrid cloud solution easy to implement. The author suggested other building blocks that included specifications of efficient hardware, UEC building and configuration, network requirements that are suitable for private and small organization.

The similarities and differences of the identified works with our presented eco-efficient building blocks are that; both work addressed TC challenges. Likewise, both work focused on cost effective cloud solution where free and open source cloud infrastructure has been preferred. The difference is that; our building blocks encompassed use of thermal VM consolidation and Green aware power sources in building private data center that suits HLIT.

4. Conclusion and Future Work

In this chapter, we have leveraged technology, environment and infrastructure to form eco-efficient and cost effective cloud computing building blocks for HLIT. The building blocks examine the basic consideration that are important in ensuring: 1) challenges that are in HLIT traditional computing are addressed in academic cloud framework; 2) Challenges that have already been presented in cloud computing framework including huge power consumption and high carbon emission are addressed in academic eco-aware framework; 3) academic framework takes advantage of environment conditions in minimizing power utilization. To ensure that stated purposes are met we identified six environments, Technology and Infrastructure building blocks. We have analyzed the nature of power to be used to power cloud data center that consider green power availability and its performance implications to cloud operations. We have taken a look on cloud deployment model and data center location that consider power sources that are available in each identified region. Next we have considered ambient climatic conditions and data center cooling. In our approach, we have explored best cooling practices that can be exploited to lower non IT facility power consumption in data centers. Besides, we have observed how ambient temperature affects free cooling. We came up with model that can enhance free cooling practice and that is in accordance with ASHRAE (2008) guidelines.

Our focus in this work was on eco-efficient but we cannot have efficient cloud without considering service delivery

infrastructure. Therefore, we have considered blocks that ensure quality of service and cloud efficient measurement. Cloud computing services are provisioned over the internet, high bandwidth connectivity as important criteria to locate a data center. We examined a network connection that can support cloud infrastructure. The presence of NICTBB in many regions in Tanzania makes data center zoning architecture across multiple geographic locations feasible. The quality of service and tradeoffs caused by virtualization has been described; quality of service consideration gives consciousness on performance and SLA violation when consolidating virtual machine.

Lastly, we have considered software necessary for building cloud computing for HLIT. Free-Open source software has been trusted in our work due to its flexibility and compatibility across multiple hardware settings. OpenStack gives many programming extensible features that can be used to create green resources cloud allocator that is suitable for a proposed zoning architecture. Furthermore, it allows cloud developers to create and manage cloud services that are distributed in a wide geographic area.

In this chapter, we have identified and discussed HLIT eco-efficient cloud building blocks and a possible cloud deployment model, i.e. Hybrid cloud has been proposed. Zoning architecture is suggested data center location strategy, where private data center will be built in a region that meets eco-efficient requirements such as availability of green power sources and ambient temperature that can be used for free cooling. In the anticipated architecture, seasonal climatic condition variation presents challenges and opportunities in free cooling strategy. Moreover, unpredictable workloads in a data center present a cloud service provisioning challenge. Thus, there has to be a VM consolidation mechanism that considers the challenges. Our future work, therefore, is to create green aware consolidation heuristic that fits in the described environment. The heuristic will consider green aware power sourced data center, and free cooling in virtual machine consolidation to reduce data center power consumption and carbon footprints. The heuristic will also optimize power consumption and carbon emission in the cloud data center.

References

[1] A. Singh and M. Hemalatha, "Cloud Computing for Academic Environment," *International Journal of Information and Communication Technology Research*, vol. 2, no. 2, pp. 97-101, 2012.

[2] M. Mircea and A. Andreescu, "Using Cloud Computing in Higher Education: A Strategy to Improve Agility," vol. 2011, 2011.

[3] M. Mircea, "SOA,BPM and Cloud Computing : Connected for Innovation in Higher Education," in *IEEE International conference on Education and Management Technology ICEMT*, 2010.

[4] R. Mero and J. Mwangoka, "Road Map towards Eco-efficient Cloud Computing Adoption in Higher Learning Institutions in Tanzania," Pan African International Conference on Information Science, Computing and Telecommunications (PACT 2014) Arusha, 2014.

[5] J. Pagare and A. Koli, "Energy-Efficient Cloud Computing: A Vision, Introduction, and Open Challenges," *International Journal of Computer Science and Network(IJCSN)*, vol. 2, no. 2, pp. 96-102, 2013.

[6] M. Kaplan, W. Forrest and N. Kindler, "Revolutionizing Data Center Energy Efficiency," McKinsey & Company, 2008.

[7] Z. Pantić and M. Babar, "Guidelines for Building a Private Cloud Infrastructure," Copenhagen, Denmark, 2012.

[8] U. Mandal, M. Habib, S. Zhang, M. Tornatore and B. Mukherjee, "Greening the Cloud Using Renewable-Energy-Aware Service Migration," Davis, 2013.

[9] Worldenergyoutlook, "World energy outlook," 2008.

[10] IndexMund, "World Energy Report," Index Mund inc, 2010.

[11] C. Wolfram, O. Shelef and P. Gertler, "How Will Energy Demand Develop in the Developing World?," 2012.

[12] M. Albaijat, "Optimal Wind Energy Intergaration in Large-sxale Electric Grids, Ph.D dissertation," UC David, chicago, 2013.

[13] S. Saidhbi, "A Cloud Computing Framework for Ethiopian Higher Education Institutions," *IOSR Journal of Computer Engineering (IOSRJCE)*, vol. 6, no. 6, pp. 1-9, 2012.

[14] D. Bouley, "Estimating a Data Center's Electrical Carbon Footprint. Schneider Electric – Data Center Science Center," *White Paper*, no. 66, 2012.

[15] TheGreenGrid, "Data center efficiency and It equipment reliability at Wider operating Temperature and humidity Ranges," *Green Greed Whitepaper*, no. 50, 2012.

[16] ASHRAE, "Second edition of the Thermal Guidelines for Data Processing Environments.," ASHRAE , newyork, 2008.

[17] ASHRAE, "2011 Thermal Guidelines for Data Processing Environments â€“ Expanded Data Center Classes and Usage Guidance. White paper," ASHRAE, Newyork, 2011.

[18] HP, "Applying 2011 ASHRAE data center guidelines to HP ProLiant-based facilities," White paper, 2012.

[19] Energystar, "energystar.gov," 2014. [Online]. Available: http://www.energystar.gov/index.cfm?c=power_mgt.datacenter_efficiency_economizer_waterside. [Accessed 4 April 2014].

[20] Z. Potts, "Free Cooling Technologies in Data Centre Applications," 2011.

[21] D. Atwood and J. Miner, "Reducing Data Center Cost with an Air Economizer.," Intel Information Technology., 2008.

[22] Rumsey-Engineers, High Performance DataCenters a Design Guidelines Sourcebook, Pacific Gas and Electric Company, 2006.

[23] A. Beloglazov, J. Abawajy and R. Buyya, "Energy-Aware Resource Allocation Heuristics for Efficient Management of DataCenters for Cloud Computing," *Future Generation Computer Systems (FGCS)*, vol. 28, no. 5, pp. 755-768., 2012.

[24] J. Hurwitz, "The Role of the Operating System in Cloud Environments," *White paper*, 2011.

[25] M. Reilly and M. Cearra, "Opennebula and The Xen Hypervisor," 2012.

[26] Cloudstack, "Cloudstack.apache.org," 2014. [Online]. Available: http://Cloudstack.apache.org/docs/en-US/Apache_CloudStack/4.0.0-incubating/html-single/Admin_Guide. [Accessed 4 April 2014].

[27] K. Suryawanshi and S. Narkehde, "A Study of Green ICT and Cloud Computing Implementation at Higher Technical Education Institution," *IJARCET*, vol. 1, no. 8, pp. 377-382, 2012.

[28] J. Ward and A. Barker, "A Cloud Computing Survey: Developments and Future Trends in Infrastructure as a Service Computing," *arXiv preprint arXiv:1306.1394*, 2013.

[29] W. Voorsluys, J. Broberg, S. Venugopal and R. Buyya, "Cost of virtual machine live migration in Clouds: A performance evaluation," in *in Proceedings of the 1st International Conference on Cloud Computing (CloudCom)*, 2009.

[30] VMware, "A Guide to Large-scale Enterprise VMware View 3 and VMware View 4 Deployments," VMware, Inc, 2010.

[31] E. Uyigue, M. Agho, A. Edevbaro, O. Godfrey, O. Uyigue and O. Okungbowa, "Energy Efficiency Survey in Nigeria. Community Research and Development Centre," Community Research and Development Centre, Edo State, Nigeria, 2009.

[32] SPEC, "Standard Performance Evaluation Corporation," 2014 . [Online]. Available: http://www.spec.org/power_ssj2008/. [Accessed 3 jun 2014].

[33] L. Shang, L.-S. Peh and N. K. Jha, "Dynamic voltage scaling with links for power optimization of interconnection networks," in *In: Proceedings of the 9th international symposium on high performance*, 2003.

[34] T. Samir, "A Roadmap for Transitioning an Information Assurance Program and Others to," *International Journal of Information and Communication Technology Research*, vol. 1, no. 3, pp. 128-138, 2011.

[35] P. Ranganathan, P. Leech, D. Irwin and J. Chase, "Ensemble-level power management for dense blade servers," in *in Proceedings of the 33rd International Symposium on Computer Architecture (ISCA)*, 2006.

[36] C. D. Patel, C. Bash and A. Beitelmal, "Smart cooling of data centers," Google Patents, 2003.

[37] J. Pagare and A. Koli, "Energy-Efficient Cloud Computing: A Vision, Introduction, and Open Challenges," *International Journal of Computer Science and Network*, vol. 2, no. 2, pp. 96-102, 2013.

[38] M. Myo and T. Thein, "Efficient Resource Allocation for Green Cloud Data Center," in *3rd International Conference on Computational Techniques and Artificial Intelligence(ICCT)*, 2014.

[39] S. Mrdalj, "Would cloud computing revolutionize teaching business intelligence courses," *Issues in Informing Science and Information Technology*, vol. 8, 2011.

[40] R. Mero and J. Mwangoka, "Building Block for Eco-efficient Cloud Computing Framework for Higher Learning Institutions in Tanzania," *Unpublished*, 2014.

[41] P. Mell and T. Grance, "The NIST Definition of cloud computing," 2011.

[42] C.-C. Lin, P. Liu and W. J-J, "Energy-Aware Virtual Machine Dynamic Provision and Scheduling for Cloud Computing," in *2011 IEEE 4th International Conference on Cloud Computing*, 2011.

[43] D. Kliazovich, P. Bouvry and S. Khan, "DENS: Data Center Energy-Efficient Network-Aware Scheduling," in *IEEE/ACM International Conference on Green Computing and Communications (GreenCom) & International Conference on Cyber, Physical and Social Computing (CPSCom)*, 2010.

[44] P. Kish, "PUE Standards for Energy Efficient Data Centers on the Horizon," 2013.

[45] A. Imenez-Castellanos, G. de la Calle, R. Alonso-Calvo, R. Hussein and V. Maojo, "Accessing advanced computational resources in Africa through Cloud Computing," *Computer-Based Medical Systems (CBMS)*, pp. 1-4; 20-22, 2012.

[46] J. Hamilton, "ooperative expendable micro-slice servers(CEMS): low cost, low power servers for Internet-scale services," in *CIDR Conference*, 2009.

[47] X. Fan, W. D. Weber and L. A. Barroso, "Power provisioning for a warehouse-sized computer," in *in Proceedings of the 34th Annual International Symposium on Computer Architecture (ISCA)*, 2007.

[48] S. Esfandiarpoor, A. Pahlavan and M. Goudarzi, "Virtual Machine Consolidation for Datacenter Energy Improvement," 2013.

[49] eia, "International Energy Outlook 2013," U.S departiment of energy 1000 independent Av, SW, Washinton DC, 2013.

[50] Cisco, "Cloud 101: Developing a Cloud-Computing Strategy for Higher Education white paper Cloud 101," 2012.

[51] M. Cardosa, M. Korupolu and A. Singh, "Shares and utilities based power consolidation in virtualized server environments," *in: Proceedings of the 11thIFIP/IEEE Integrated Network Management*, 2009.

[52] M. Bluckburn, "Five ways to reduce data center server power consumption. The Green Grid," 2008.

[53] A. Beloglazov, R. Buyya, L. Choon and Z. Albert, "Taxonomy and Survey of Energy-Efficient Data Centers and Cloud Computing Systems," *Future Generation Computer Systems (FGCS)*, vol. 1, no. 2, pp. 1-52, 2010.

[54] Australia, "Australian Government Data Centre Strategy 2010-2025. Better Practice Guide: Data Centre Cooling.," Australia Gov, Australia, 2013.

[55] 42u.com, "www.42u.com," 2014. [Online]. Available: http://www.42u.com/cooling/economizers/economizers.htm. [Accessed 04 April 2014].

[56] R. Suryawanshi, P. Choudhary and Naidu, "An Analysis and Implementation of Cloud Computing at Higher Technical Education," *International Journal of Computer Applications and Business Intelligence (IJCABI),* vol. 2, pp. 13-19, 2012.

[57] N. Ajiths and M. Hemalatha, "Cloud Computing for Academic Environment," *International Journal of Information and Communication Technology Research,* vol. 2, no. 2, pp. 97-101, 2012.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 171-174, 2018, ISSN:-2319–8656

A Secure MSSS Scheme and AES Encryption over Cloud Data

Sreelakshmy D Unni
PG Scholar
Department of Computer Science and Engineering
Mangalam College of Engineering
Kottayam, Kerala
India

Neethu Maria John
Associate Professor
Department of Computer Science and Engineering
Mangalam College of Engineering
Kottayam, Kerala
India

Abstract: In this era Cloud plays a vital role in storage of all type of data. Thus the availability of data also increased. The data can be subscribed and maintained comfortably. It also solves the problem of excess computation cycles, software updates and handling high loads of data. AES is the encryption techniques used by worldwide. Most Significant Single Keyword Search (MSSS) is efficient search that uses Most Significant Digit (MSD) Radix Sort. The main challenge facing are security of data in Cloud. In this we propose Secure MSSS Scheme and AES Encryption over Cloud Data. AES is a symmetric encryption block cipher which allows different key length. Encryption is performed by interchanging characters of key and data. In this we are using a private cloud. The data uploaded to cloud is stored as encrypted file. Encryption performed using AES encryption algorithm. The data stored in the cloud is accessed by the allowed users of private cloud and searching of data done using MSSS. The MSSS scheme is faster soring array strings. Encryption solves the problem of security to an extent. AES will have 10, 12, 14 rounds of encryption.
Keywords: Cloud computing, AES Encryption, MSSS, Radix sort, Security, Symmetric.

1. INTRODUCTION

To get a pool of computing data owned and maintained by a third person via internet is termed as Cloud computing. The cloud includes network, storage, hardware and interfaces provide user to access computing data, services on demand those are independent of the location. The storage of user data which is already stored in some other locations. Cloud storage of data is like renting the asset according to your requirements. So that it avoid buying the whole infrastructure to perform a particular process. It mainly uses remote services through networks using various type of resources. By using cloud the user is capable of using maximum computing of data with the minimum hardware requirements. Location independency, scalability, device independency are the main advantages of using cloud. Private clouds are more secure than public clouds, it is a challenge to store data without keeping private information in cloud. So that we are encryption the data in cloud.

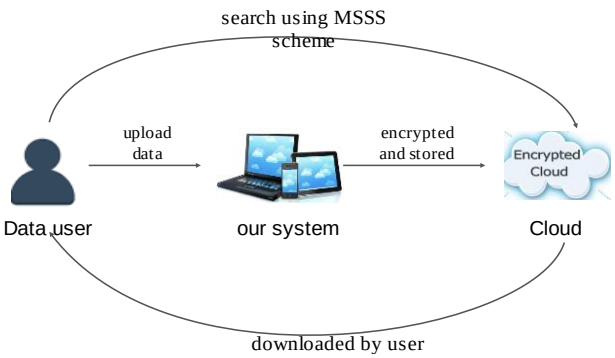


Fig 1: Overview of Proposed System

The encryption algorithm we are using here is AES Encryption algorithm. All of the organizations have their own private data's to keep secured, then we use encryption. AES is efficient encryption algorithm and is unbreakable when compared to other algorithms. AES is symmetric key encryption with separate key is used to for both encryption and decryption. The plain text chosen will be of length 64bytes to 52 bytes and 6 rounds with a complexity 2 126.8 encryptions. Key size of AES can be varied such as 128, 192, and 256. In this public key is used to perform encryption and private key used to perform the decryption.

2. RELATED WORKS

The encrypted and decryption are performed using the same secret key and data is stored in the disk. The algorithm used in this system is Advance Encryption Standard (AES). AES uses key size 128,192 and 256. The number of rounds 10, 12, and 14, respectively. The encryption is done by interchanging some of the characters with key and data in it. The main feature of the system is disabling the delete option in the right click menu for the encrypted files. To provide security to all these confidential data on the desktop by converting the plain text to cipher text when the file is encrypted. AES is unbreakable when compared to other algorithm. The confidential data on a desktop are encrypted using AES with a secret key to secure the files. Once the file is encrypted using secret key then the user has to enter the same secret key for the process of decryption. If the secret key entered is matching with the encryptions secret key, then file will be decrypted successfully else, file cannot be decrypted message is displayed [1].

The cloud deployment models, service delivery models of cloud computing, characteristic of cloud, cloud computing

adopting risks, technology, cloud computing security problem and data encryption using RSA, DES and AES[2]**.** Now the 4G technologies and the development of 5G technologies profoundly changed people's life with wireless devices. Huge number of mobile applications produce sensitive data in many fields and most data stored in cloud. The complexity to search data over encoded information for wireless devices without strong computational capability. In this AES, DES, RSA are described to provide security. Cloud computing is the technology most used. It is a good solution for all of them because of personnel storage has not be used or this is less expensive. Cloud computing vulnerabilities are security issues and loss of data [7]. The classical solutions where threats come from two known sources inside or outside the network [2]. In this the threats originate from different sources because the data stored in cloud are from different sources. The different models of cloud and risk factors when adopting cloud computing, technology, security issues in cloud and data encryption using RSA, DES and AES [2].

The secure ranked multi-keyword search is multi-owner model. The cloud servers have to perform secure search without knowing the actual data of both keywords [3]. Efficiency of our proposed schemes experiments on real-world datasets are running. In this cloud servers are systematically construct a novel secure search protocol which helps to secure search without knowing the actual value of both keywords and trapdoors. The different data owners use different keys to encrypt their files and keywords [3]. A query is used to generate keys to authorized keys user can issue without knowing secret keys of these different data owners. Different type of works enables authorized data users to be secure, confidentiality, efficient search over multiple data set**.** To get search results and rank the system privacy keywords and files, we propose a novel Additive Order and Privacy Preserving Function family [3].Thus this approach is efficient in performance wise compared to very large data set and keyword set.

3.PROPOSED METHODOLOGY

Now a days many enterprise store and outsource data through cloud. By this the sensitive data's stored in cloud are much secure. The data have to keep secure is a very big problem. So that data's are encrypted and stored in cloud, data's such as financial, personal and government data's. From the encrypted stored data the user have to find their on data using MSSS. The user will request for the data and get the matching data without much knowledge about the encrypted cloud [4].

All files are encrypted, storage and searching is not a simple job in very large systems [9]. The cost of searching have been reduced without affecting the search request of the data stored in cloud. With the high security the document have to select accurate keyword search over encrypted cloud [10]. Unauthorized entitles or other service providers can't able to access data from this cloud. The MSSS will reduce the searching overhead and time over the AES encrypted cloud data. The index generation time is reduced to O(Nt*3) retrieval of data from encrypted cloud with top k single keyword [4] .

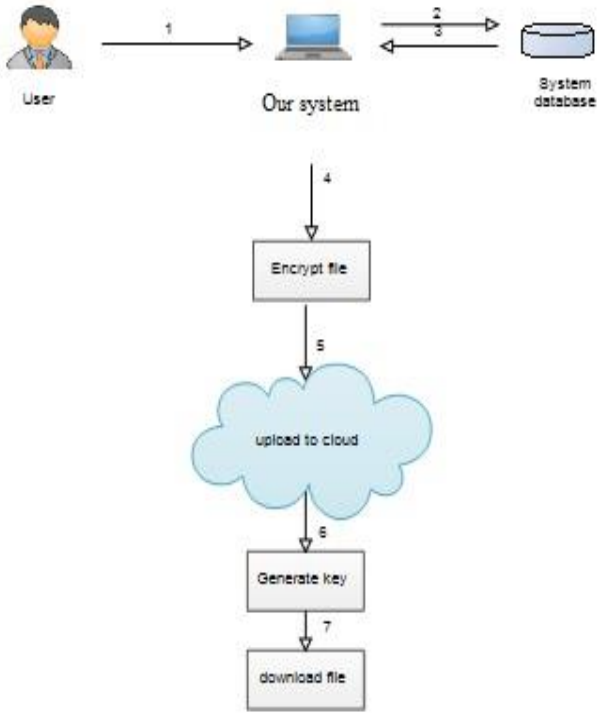


Fig 2: System Architecture

In the system architecture the user enters data into the system. Only the authorized user in the system can access this system. This system stores all passwords in the database in encrypted format. The data stored in the database is uploaded to cloud after performing the encryption using AES. When the user searches an encrypted file in cloud. The data file downloaded from cloud with a secret key send by system administrator to users email. This improves the security of the system and unauthorized access to the data files. The searching scheme here used is MSSS. The Steps are

1. An authorized user uploads data file into the system.
2. The system stores the data file in Data base to create a unique key for the data file.
3. The System administrator retrieve data file from base data base.
4. Then the System administrator perform the encryption of data file by AES encryption algorithm.
5. The encrypted file is uploaded to the cloud.
6. When a user searches the file in the cloud using MSSS search scheme, and request is send to administrator to download the data file.
7. The system administrator sends a secret key to the users mail and using that mail the user can download the data file

1.MSSS

Algorithm 1: Most Significant Multi-keyword Search (MSSS)

Initialization Phase
input : A set of n Data Files F = (f1, f2, . . . , fn)
output : Index file generated from extracted keyword I
Function: Build Index(K, F)
for fi ← 1 to n do
each file fi ∈ F ;
Scan F and Extract the distinct word in fi, denoted as a W = (w1, w2, w3, . . . wn,) ; Normalized and filter the stop words from W ;
for j ← 1 to m do
each file wi ∈ W ;
1) Calculate the Score S for each keyword wi according to equation 1;
2) MSD() to sort the Index I;
3) Compute α(wi) for each keyword wi according to equation 2;
4) Store the hid(fi)||α(wi)||Si as an element in the posting list of I' ;
5) Encrypt the Index file I';
6) Replace I' with I''
return I'';

1.1Radix Sort

This algorithm arranges string in ascending or descending order. The algorithm process the string of grouping keys which have the same significant position and value. The two type of radix sort are LSD and MSD. Here we are using MSD (Most Significant Digit).

1.2 MSD

MSD uses lexicographic ordering which is suitable for sorting strings such as word or fixed length integer.MSD radix sort starts the string processing from right side that is opposite to LSD. The MSD stops processing by rearranging reaches the prefix of the key MSD sort uses multiple level of bucket.

2. AES

AES is a symmetric key encryption technique which consist of 4 encryption stages. The stages are Substitution Bytes, Shift Rows, Mix Columns, and Add Round Key. AES require block size to be 128 bits, the state array of different size block has only 4 rows in other ciphers. The number of columns depend on size of the block. The data on cloud is encrypt using secret key with AES as encryption algorithm. The user have to give 16 bytes of secret key twice to uniform the secret key [1].

Table: AES Versions

Version	Key Length	Block Size	No: of Rounds
AES -128	4	4	10
AES -192	6	4	12
AES -256	8	4	14

Once a file is encrypted using a secret key, the decryption have to be performed using the same secret key which have been used for encryption. If the secret key changes or misplaced then the decryption cannot be performed. The deletion of encrypted file can be also performed in this cloud. In this we have to select the file for encryption. The file selected have to upload to cloud. Then the file have to be perform encryption and uploaded. Then the file is stored in the cloud. When the user needs the file we search the file using MSSS and download the file with the help of a key that is given to authorized user. Only by inserting the key we can download the file from the cloud.

The 4 Stages of AES [5]

1. Sub Bytes transformation is a nonlinear byte substitution for each block of data.

2. Shift Rows transformation cyclically shifts the bytes within the block.

3. Mix Columns transformation groups 4bytes together forming 4-term polynomials with a fixed polynomial mode.

4. Round Key transformation adds the round key with the block of data

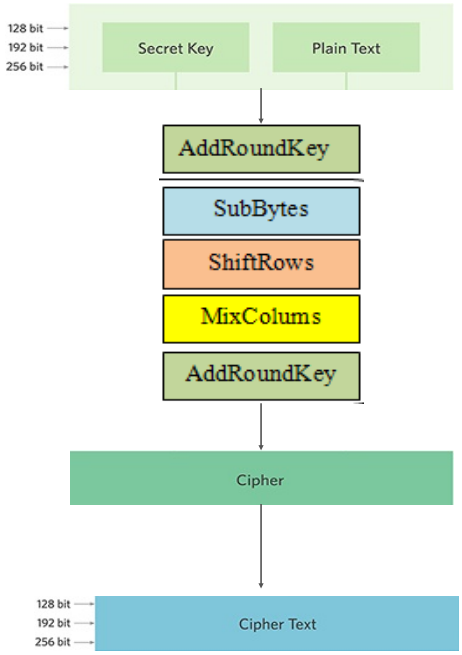


Fig 3: AES encryption steps

4. EXPERMENT AND RESULTS

The three encryption algorithms are symmetric block cipher. The AES uses 128,192,256 bits key length which can use variable length keys [8]. The DES uses 56 bit key length and triple DES uses 168 and 112 key length used by Triple DES [6].Block size of data also used by AES is 128, 192, 256 bits. DES uses 64 bit data block size. Triple DES also use 64 bit of data.There is graph Fig 4 which compares the security or usage of these three algorithms. From this we can conclude that AES is better than DES and Triple DES. The MSSS scheme which use index storage space of cloud server which

reduced and it creates an index storage of files [4]. So the search time will be reduced over the encrypted cloud. The searching time of MSSS is efficient compared to Greedy Depth First Search algorithm shown in Fig5. Storage overheadand computation time is reduced. Real data which reduces index store and keyword search time over the encrypted cloud.

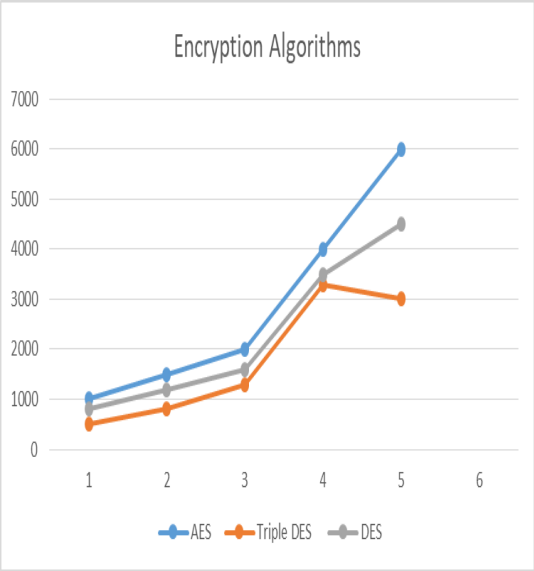


Fig 4: Comparison of encryption algorithm

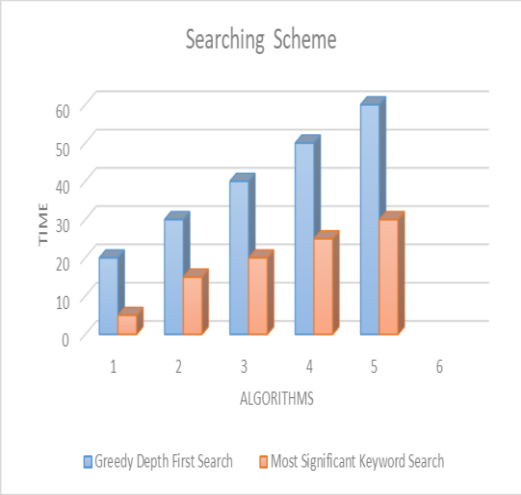


Fig 5: Comparision of Searching schemes

5. CONCLUSION

Now a days the data security issues are increasing day by day in cloud. Searching data in the encrypted cloud is a complex problem. In this for encryption we are using AES encrypted cloud and MSSS searching scheme for searching data. The combination of AES and MSSS will have high efficiency with the data security, storage and efficiency in searching the data's in cloud. In this Radix Sort, MSD is used. for searching of stored data over encrypted cloud. The performance of the system is improved as the searching time required is less compared to other searching algorithms. The AES encryption is much secure than the other encryption algorithm. So that the system will be highly efficient and data is secure in the cloud

REFERENCES

[1] Securing Files Using AES Algorithm. Aditya Rayarapu, Abhinav Saxena, N.Vamshi Krishna, Diksha Mundhra.

[2] A Survey on Security Using Encryption Techniques in Cloud Gaurav Jain, Vikas sejwar P. G. Scholar.

[3] A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEETavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] MSSS: Most Significant Single-keyword Search over Encrypted Cloud Data Raghavendra S, Geeta C M, Shaila K, Rajkumar Buyya, Venugopal K R, S S Iyengar, L M Patnaik.

[5]https://www.vocal.com/cryptography/advanced encryption-standard-aes.

[6] A Study of Encryption Algorithms AES, DES and RSA for Security by Dr. Prerna Mahajan & Abhishek Sachdeva IITM, India.

[7] Secure User Data in Cloud Computing Using Encryption Algorithms Rachna Arora, Anshu Parashar Research Scholar, HCTM, Kaithal, Haryana (Associate Professor, HCTM, Kaithal, Haryana.

[8] Advanced Encryption Standard (AES) Standard (AES) Raj Jain Washington University in Saint Louis Saint Louis, MO 63130 Jain@cse.wustl.edu.

[9] Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data Ning Cao†, Cong Wang‡, Ming Li †, Kui Ren ‡, and Wenjing Lou† †Department of ECE, Worcester Polytechnic Institute.

[10] A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data. Cengiz Orencik∗, Murat Kantarcioglu† and Erkay Savas∗ ∗Faculty of Engineering and Natural Sciences Sabanci University, Istanbul, 34956, Turkey† Department of Computer Science The University of Texas at Dallas Richardson, TX 75080, USA.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 175-184, 2018, ISSN:-2319–8656

Intrusion Detection against DDoS Attack in WiMAX Network by Artificial Immune System

Mehrafrooz Reyhani
Department of Computer Science, Yazd Branch, Islamic Azad University, Yazd, Iran

Vahid Ayatollahitafti*
Department of Computer Science,Taft Branch, Islamic Azad University,Taft,Yazd, Iran

Mohsen Sardari Zarchi
Department of Computer Engineering, Meybod University, Meybod
Iran

Abstract: IEEE 802.16, known as WiMax, is at the top of communication technology because it is gaining a great position in the wireless networks. In this paper, an intrusion detection system for DDOS attacks diagnosis is proposed, inspired by artificial immune system. Since the detection unit on all subscriber stations in the network is WIMAX, proposed system is a fully distributed system. A risk theory is used for antigens detection in attack time. The proposed system decreases the attack effects and increases network performance. Results of simulation show that the proposed system improves negative selection time, detection Precision, and ability to identify new attacks compared to the similar algorithm.

Keywords: **WIMAX network, Artificial Immune System, DDOS Attack**

1. INTRODUCTION

Computer networks are changing and developing very quickly either in architecture context or software context of the network and these changes affect the network traffic. Therefore, the examination of the network traffic has always been discussed by researchers. WiMAX network is very dynamic and it is possible that the topology between stations be different from physical network, also the shared files can be replaced according to the topology of wireless network. Therefore, traffic in WiMAX network can be examined from different aspects such as, the distribution of packet entrance in time unit, the interval between packet entrance and the distribution of packet size. If the number of these packets exceeds the threshold value, network resources will be saturated, because the stations in WiMAX network leave the network or join it in anytime[1,2]. Therefore, they will be exposed to DDoS attacks and such behaviors should be detected and prevented. In order to prevent, detect, encounter and stop attack, security should be recognized and created over the network in the first stage. The first security level is to prevent intrusion and intrusion detection system is the second defensive line. The main strategy to solve security problem in WiMAX network is to use intrusion detection system. By using these strategies, it is possible to detect suspicious ways and potential attacks. As current systems are continuously changing and the strategies to intrude them are also gradually changing, it is essential that intrusion detection system be dynamic over time.

Two noticeable factors in vulnerability of WiMAX network are the flooding sent of message and its decentralized nature [3]. If DDoS attack is managed, it can be controlled in other wireless networks. As DDoS attack contains a large number of distributed machines, the development of defensive nodes would be effective in discovering DDoS attack. Collaborative discovery requires that heterogeneous stations be adhered and it guarantees high scalability and security against attacks [4,5].

Considering the main features of distributed systems and also examining the different mechanisms of human immune system can reveal some similarities between these two seemingly different contexts. Regarding these similarities, we are inspired by human immune system to identify effective intrusion in distributed systems. In the suggested system the combination of artificial immune system algorithms are used. This system follows its operation in several levels with heterogeneous functions of stations.

The rest of this paper is organized as follows. In section (2), we describe the intrusion detection system which is related to this context and we briefly introduce intrusion detection by inspired from artificial immune system. In section (3), includes a brief analysis of suggested intrusion detection system, the results and details of our dataset. Finally in section (4), the paper is concluded with a discussion of our proposed intrusion detection system and artificial immune system.

2. REVIEW OF LITARETURE

The majority of researches examining attacks just focus on one system but the attacker's purpose is to sabotage several systems. Since the suggested system is based on human immune system, in this section we outline previous studies about the intrusion detection system of WiMAX network and also researches that exploit human immune system to secure computer networks.

INTCD [6] is a distributed system based on neural networks for detecting network traffic anomalies and for dynamically modifying the network resource access policies. Initial data of network traffic is examined and any suspicious behavior is discovered. One of the advantages of this system is flexibility but before doing anything, some data should be thought to this system.

DD-police [7] protects wireless network against DoS (Denial of Service) attack. In this model, stations supervise their neighbors' traffic. If a node receives a lot of requests from its neighbor, this neighbor will be identified as a suspicious node. Scalability and frequency of sending neighbors' list are two factors that should be mentioned in this model. In wireless network with its high dynamic nature, nodes leave and join a lot, and also increase in the frequency of neighbors' list raises the system's overload.

In the context of exploiting the features of human immune system for the security of computer networks, Forrest performed the first researches to discriminate between self and nonself in network artificial immune system. Then Hofmeyr [8] designed an artificial immune system called ARTIS. This system is not very efficient because collaboration and information exchange among nodes is not considered and intrusion detection is done separately in each computer.

LISYS [9] is one of the first structures for artificial immune systems that is designed for a simple local network and can learn network traffic and identified anomaly traffic.

CVIS [10] has some characteristics such as analyzing the discovered virus, repairing defective files and spreading the results of analysis to other local systems. Although CVIS operates in a distributed environment using the autonomous factors but scalability is its cliché problem.

CDIS [11] is also designed in artificial immune system to detect computer viruses. CDIS is a developed form of LISYS and both have the same base. The life cycle of detectors is also same. In the both of them, detectors (antibodies) are randomly produced in both. This system can detect viruses and network intrusions. CDIS is a multilayer and distributed computational immune system. One of the problems of CDIS structure is that it only analyzes and examines one packet in anytime.

The purpose of Cfengine [12] system is to automatically configure large number of systems on heterogeneous nodes. Furthermore, as long as a new discordance does not happen, the intrusion detection system is passive. In order to increase scalability, Cfengine intrusion detection system updates the average of system efficiency, the number of each service input and output connection and packet characteristic. Results of Cfengine show that danger signal potentially affects false positive rate and also memory detectors improve detection rate.

3- THE PROPOSED INTRUSION DETECTION SYSTEM

Since the proposed system contains new ideas and a combination of different algorithms are used to developed purposes, we will investigate this system from three different aspects: intrusion detection system, WiMAX network and artificial immune system.

3.1 INTRUSION DETECTION SYSTEM

As the proposed intrusion detection system is located in all subscriber station, system announces the existence of attack or intrusion to

other Base station by means of distributive BS warning. Consequently the stated system discovers the network intrusions by cooperation between SS and BS.

Intrusion detection system can be divided into two different groups: network intrusion detection system (NIDS) and host intrusion detection system (HIDS) [13,14].

NIDS is installed on the network's gateway and examines the traffic of the network from which it passes. Since BS in WiMAX network plays the role of gateway and also the role of decided in distinguishing anomaly traffic from normal traffic, the BS sends attack strategy to other BSs after identifying and proving attack.

HIDS performs on different nodes based on collecting network traffic information. These pieces of information are separately analyzed in each node and the results are used to immune the activities of the aforementioned node. Obviously the proposed intrusion detection system is located on all SS so this system performs distributive. The results, informs other nodes in WiMAX network of the existence attacker node.

To detect intrusion, the algorithms of artificial immune system such as negative selection [15] and clonal selection [16] are used. In fact, new and unknown attacks are detected. Anomaly traffic and normal traffic are distinguished using danger theory. Therefore, the proposed system is formed by the process of combining two methods. In the training phase use anomaly-based intrusion detection and in the test phase utilize signature-based intrusion detection.

By saturation of network resources in a short time and prediction of attack possibility, the node (BS and SS) in the suggested intrusion detection system warns its BSs to confront attacks. Therefore, on surrounding BS become aware of possible attack. Invaded nodes would be suspended since they are not resistant against attack and they are protected to some extent. This system has an active attitude by detecting and announcing SS and BS new behaviors.

It should be mentioned that SSs perform intrusion detection continuously but BSs would be active just by sending the Stress message from SSs.

3.2 ARTIFICIAL IMMUNE ALGORITHM

Since human immune system performs actively and distributively, artificial immune system algorithms are extremely used in proposed system to develop purpose. Here major features of human immune system are inspected to detect intrusion and how it reacts against intrusions. Then its application in WiMAX network to confront DDoS attack will be mentioned.

In the suggested system negative selection algorithm is used in training phase and its function is as follows:

Network normal traffic which contains WiMAX network packets is captured by TFN2K monitoring tools. Then it considered as a self-dataset. After that some detectors(immature detectors) are produced by random Gaussian function and by comparing these two datasets, any detectors that do not correspond to network normal traffic will be added to the detectors' list as none self-detector(mature detectors). In this stage, the number of detectors is investigated. If this number increases, the accuracy of detection goes up and computational overload increases too.

Algorithm 1. Negative selection method in training phase

Input: selfdata

Output: detectors

Use KDD dataset for normal traffic

W_{nd}: WiMAX normal dataset

W_{ad}: WiMAX abnormal dataset (detector dataset)

D: detector

D_{th}: Threshold of detector

1: **while** number of d less than D_{th}

2: d← create immature detector with uniform Gaussian random function

3: **if** W_{nd} contains d **then**

4: drop d

5: **else**

6: d insert into W_{ad}

7: **end if**

8: **end while**

After receiving each WiMAX packet, the information will be added to template. Then the size of bandwidth occupation will be examined. If it does not reach to the default threshold(70%), the template will be faded out of existence and a new template will be made.

Otherwise, the possibility of attack occurrence will be announced to connect BSs and then SS after making sure of the existence of each BS sends the template of possible attack (the structure of antigen DNA) to each BS. In this stage, SS announces the possibility of attack occurrence and distinguishes between abnormal traffic and normal traffic. SS will be suspended in a definite time span to prevent the reception of any packet or message. When this time span ends, SS will return to its initial state.

BS announce its existence to SS by receiving the possibility of attack occurrence and after receiving the template of possible attack compares that to its nonself dataset. If the template conforms to each detector, BS broadcasts it to other BSs as a detector. Then BS creates conformed detectors once again, increases their affinity and if detectors aren't conformed, BS will make them older. In either way BS examines detectors' affinity in order to change its main structure.

According to the number of conformities, detectors' situation changes from mature stage to active stage and from active stage to memory stage. In next step each detector's beneficial life time along with its kind is inspected. As each kind of detector has a definite life time, those detectors whose life time is ended are deleted from detectors dataset.

Genetic algorithm is used to improve detectors in the proposed system. This algorithm also causes variety in nonself templates in active stage, in a way that based on clonal selection algorithm, those cells that identify detector grow and those cells that are not able to identify detector die.

As SS and BS operate in a collaborative and parallel manner, SS's and BS's function are separately inspected.

Algorithm 2. Subscriber station(mobile node) Function in test phase

Input:anomaly wimax traffic

Output: template message

W_p: WiMAX Packet

BW_d: percentage of Subscriber station Bandwidth depletion

BW_{th}: Threshold of Subscriber station Bandwidth depletion

01: **While** SS is in active mode

02: T← receive features of new W_p

03: **if** $BW_d \geq BW_{th}$ **then**

04: forwards msg-stress along connected Base Station

05: **else**

06: Drop T

07: **end if**

08: **if** received msg-sressreply **then**

09: forwards T to certain Base Station

10: stand in suspend mode for time span

11: **end if**

12: **end while**

Algorithm 3. Base Station Function in test phase

Input:template message

Output: detector

T_a: Template of attack

T_c: number of conformity with Ta

T_{ttl}: time to live for every detectors

01: **while** Base Station is in active mode

02: T← receive W_p

03: **if** W_p.Type is msg_stress **then**

04: forwards msg_stressreply along subscriber station

05: **end if**

06: T_a← received msg_template

07: **if** W_{ad} contains T_a **then**

08: increment T_c

09: set T_{ttl} to zero

10: update W_{ad} with T_a

11: forward T_a along every Base Station in network

12: Run GA .Algorithm on W_{ad}

13: **end if**

14: **end while**

4. PERFORMANCE EVALUATION

We implemented intrusion detection system in WiMAX network used OPNET simulator 14.5. This version of simulator is first version that embedded 802.16 standards. Radio source in WiMAX network are consisted by time/frequency slices. The number of slices in downlink depends on related system bandwidth, frame period, downlink/uplink rate, permutations under vector (AMC, FUSC, PUSC), and protocol header (FCH, maps, preamble).

4.1 SIMULATION DATA PRELIMINARIES

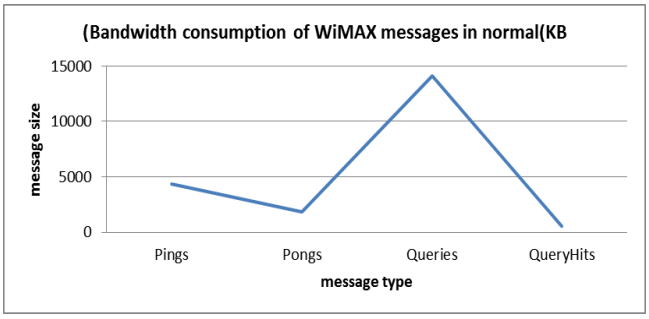
Three subnets with different numbers of nodes were used in simulation scenario that is WiMAX network with metroethernet structure. The connection between subnets is done with third layer switch, and VLAN is used to prioritize to traffic. To increase security in WiMAX network, server connection and relation between BS and metroethernet structure were considered. In this simulation, number of production packets was considered 50 packets in an hour and 300 seconds for production time. Transmission packets used IP/UDP protocols. In simulation scenario WiMAX network with metroethernet structure, number of mobile nodes in each all or even in each subnet was considered to study varios factors and their changes. System bandwidth is 2.5GHz, TDD frame period in WiMAX is equal to 5ms and ratio of downlink to uplink is . PUSC was considered in simulation. For the simplicity, protocol header consists of two fields. Number of slices in each TDD sub frame equals to NS=450. The parameters are shown in table 1.

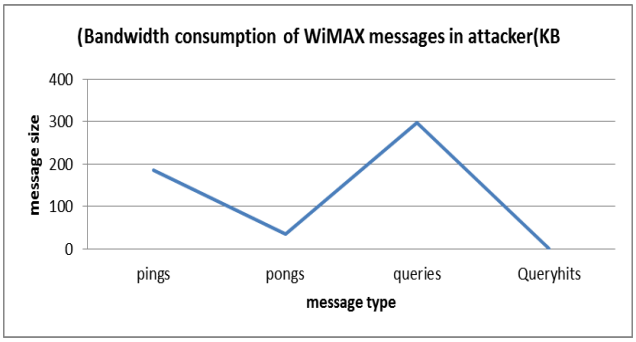
Table 1. Simulation parameters

Parameters	value
Base frequency	2.5GHz
Duplexing mode	TDD
System bandwidth	5Mbps
Propagation model	Two ray ground
Cell radius	50m
DL/UL ratio	3:2(27:18 OFDM symbols)
Frame length	5ms
PHY	OFDM
DL permutation zone	PUSC
MAC PDU size	Variable
Inter-arrival between frames	120ms
Simulation time	300s
Number of detector	75

In the early stage of simulation, the type of WiMAX message is used to form attack template. But as maximum of messages is related to Query message, an almost similar template is achieved in the definite time span and in order to prove that. Transmitted messages in WiMAX network are examined in three conditions: normal, attacker node and victim node.

When DDOS attack happened, the used bandwidth of each WiMAX messages was examined and according to various experiments on victim stations and attacker stations, the maximum consumption was related to Query message. Figure 1 proves this claim.





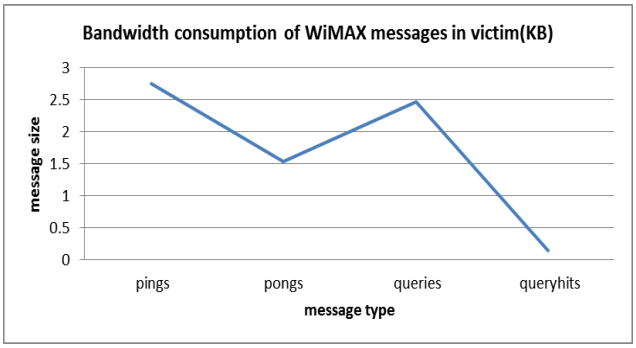
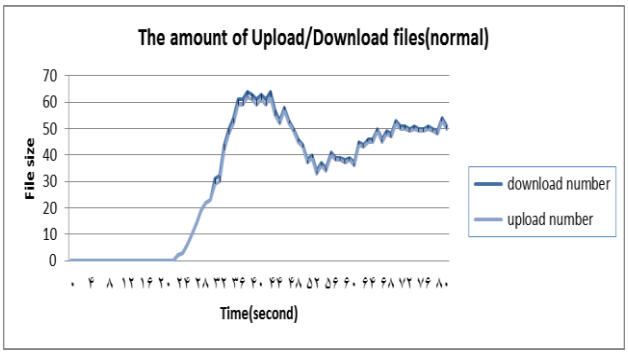
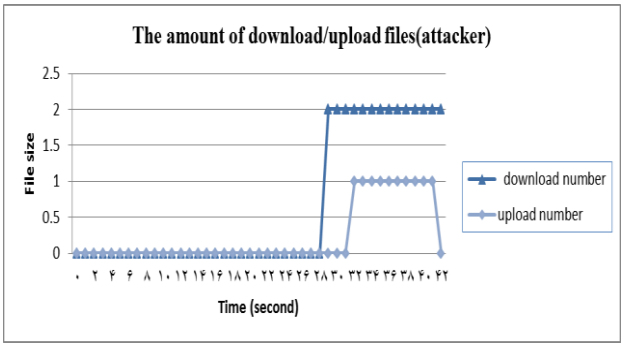


Fig.1. Bandwidth consumption of WiMAX messages in normal condition, attacker, victim.

The number of shared files is evaluated in both normal and attack conditions. In normal condition, the amount of files download and upload has approximately been equal but in attack condition the amount of download has been minimized. This is shown in figures 2. The real network in normal condition, maximum traffic is related to download shared files.





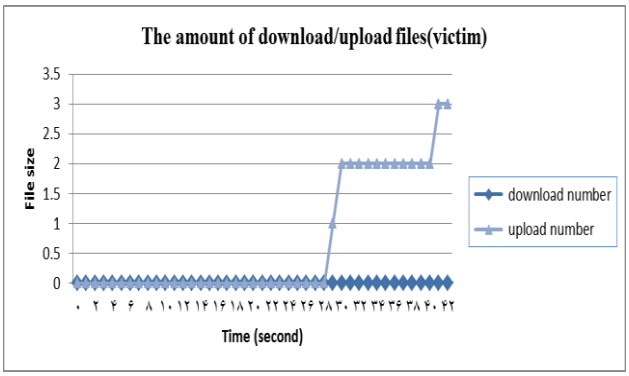


Fig.2. The amount of downloaded and uploaded files (a) normal condition (b) attack condition for attacker (c) attack condition for victim

In next step, we have formed template by factors such as source IP address, destination IP address and average of time interval between consecutive two messages. As the majority of messages are Query, recording message type is something extra. When the source IP address and the time of message sending are equal, attacker node can be identified and DDOS attack can be announced by examining the source IP address and time interval which is passed to send the packet to destination. In fact, if the IP address of messages and the time interval which is passed until packets get to destination are equal and the consumption bandwidth exceeds threshold, DDoS attack has happened.

4.2. SIMULATION RESULTS ANALYSIS

The efficiency of proposed system is analyzed based on the following criteria:

- Negative selection time

- Detection Precision
- Ability to identify new attacks

Negative selection time: Some immature detectors are produced by random Gaussian function and this dataset compares with WiMAX normal dataset. If any detectors do not match with normal traffic template, it will be added to the mature detectors' list. Output of training file is a mature detectors' dataset. The small amount of dataset used in this simulation and also the dataset which has been chosen for conformity decreases the time of negative selection in comparison to LISYS algorithm. Figure 3 shows time of negative selection in proportion to the size of training file.

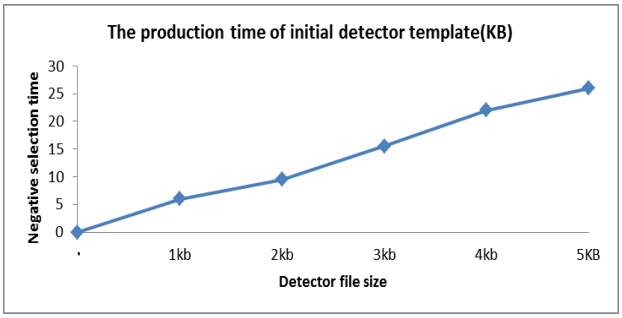


Fig.3. The production time of initial detector template.

Figure 4 Shows the time of negative selection in proportion to the number of detectors. By increasing number of mature detectors, negative selection time will be increase too but, detection precision is optimized. Because of using genetic algorithm, the time of negative selection is more beneficial than LISYS algorithm.

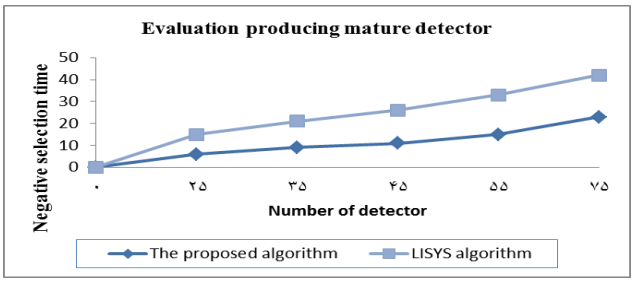


Fig.4. The production time of mature detector.

Detection Precision: In order to increase detection precision, false positive should be reduced.

These parameters include:

- The number of detectors
- The specificity of detection (the r parameters of bit matching algorithm)
- The crossover and mutation operators for genetic algorithm.

We also look at which parameters appears most important for minimizing false positives, as well as how maximizing percentage of detecting intrusions. The percentage of attack detection will be measured by proportion of discovered attack occurrences to all attack occurrences.

In fact «false positive is the sending of alarm message by intrusion detection system in the time that attack has not happened».

The proposed system is adopted to describe the tradeoff between the detection rate and false positive rate. Therefore, we evaluate the best attitude coherent to these factors for yielding optimum resolves.

a. number of detectors

To study the effect of mature detectors on the percentage of attack discovery and false positive, the parameter of activation discovery is considered 6, crossover operator 0.4 and mutation operator 0.005. These two factors are evaluated by the change in the number of detectors in the number of different conformity bits. Through increase in the number of detectors, the percentage of attack discovery goes up on the one side and the false positive increases on the other side. In a way that in all the forms of conformity bit, 75 detectors show the most efficient response for detecting attack. But due to computation over load, the number detectors are commonly not very high. In LISYS algorithm, the number of detectors is 100. Figure 5 proves this.

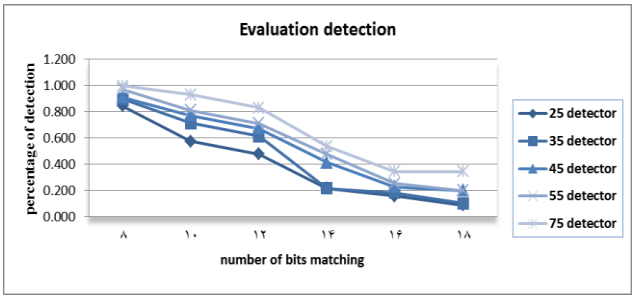
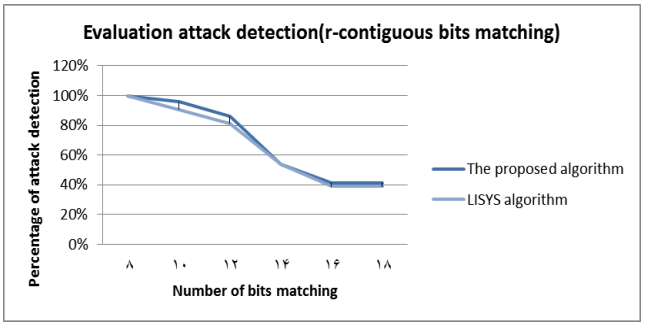


Fig. 5. Evaluation detection with different number of detector

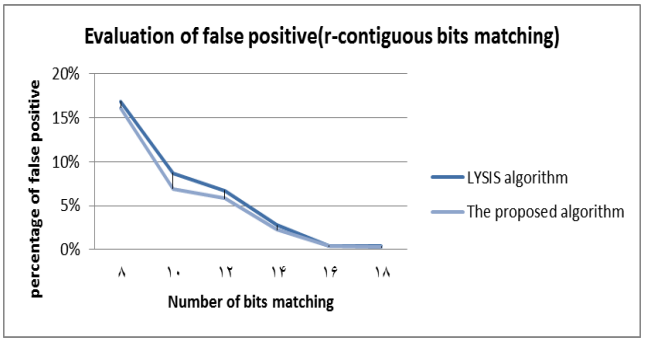
b. parameters of bit matching algorithm

Some detectors in this system usually implement as strings, whose function is to classify new strings as normal or abnormal by matching them in some forms. The perfect matching is rare in the immune system. So, we use a partial matching rule is known as r-contiguous bits matching. Under this rule, two strings match if they are identical in at least r contiguous locations.

Our observations in figure 6 show that immune system as inspiration for detecting intrusion is the best approaches. In particular, the r-contiguous bits matching rule is proposed in LISYS and we use it for our system. To study the effect of mature detectors on the percentage of attack discovery and false positive, the parameter of activation discovery is considered 6, crossover operator 0.4 and mutation operator 0.005. These two factors are evaluated by the change in the number of detectors in the number of different conformity bits. The number of strings a detector matches increases exponentially as the value of r decreases. For example, 8 conformity bits is the best resolve for attack detection rate but is the worst result for false positive rate. After checking these factors, we elect 8 conformity bits and LISYS algorithm elect the number, too.



(a)



(b)

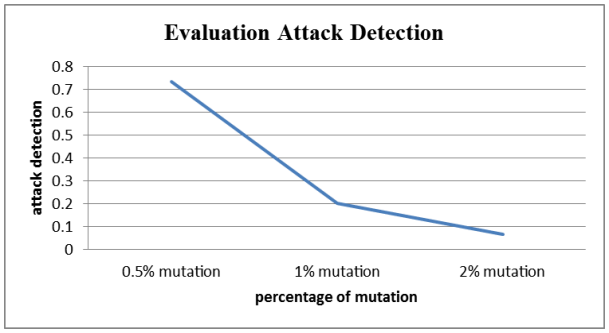
Fig.6. Evaluation attack Detection and Evaluation false positive

C. Crossover and mutation parameters

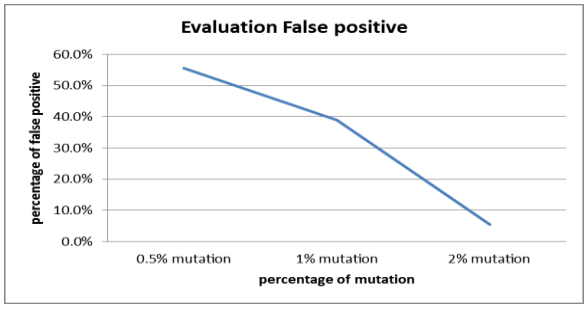
As 100 attacks are discovered, generation production happens once, but with occurrence of each attack, homeostasis process is defined, in other words the detectors that should be thrown away or remain in the detectors set are defined.

In this condition the number of detectors is considered in the best state which is 75. The highest detection percentage is found by the number of bit conformity and activation threshold and then mutation rate is examined and finally the best mutation rate is computed for the highest discovery percentage.

As 73% of the best attack detection responses have the mutation rate of 0.005 and also in the examination of false positive, 56% of the lowest false positive is related to mutation rate of 0.005, therefore in the suggested system the same mutation rate is used.



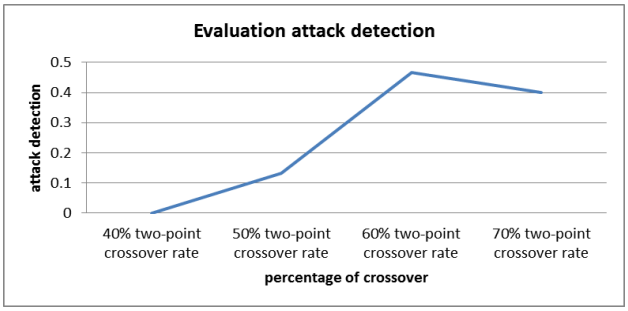
(a)



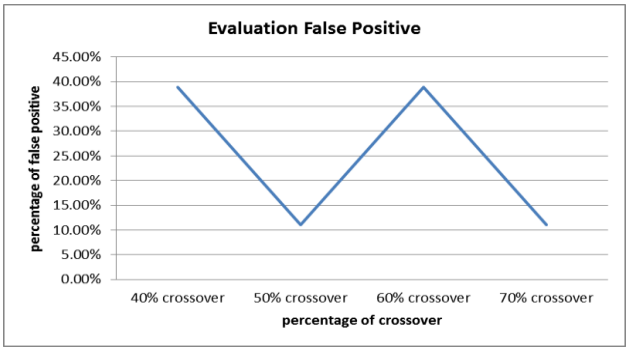
(b)

Fig.7. Evaluation attack detection and evaluation false positive

In this condition the number of detectors is considered in the best state which is 75. The highest detection percentage is found by 12 conformity bits, activation threshold and then crossover rate is examined and finally the best crossover rate is computed for the highest discovery percentage and the lowest false positives percentage. As 47% of the best attack detection responses have the crossover rate of 0.6 and also in the examination of false positive, the lowest false positive is related to crossover rate of 0.4 and 0.6, therefore in the suggested system the 0.6 crossover is elected.



(a)



(b)

Fig.8. Evaluation attack detection and evaluation false positive

Ability to identify new attacks: As the training phase of this system is performed on all nodes and also in the stage of BS checking, with the attack detection, its pattern is sent to other BSs, therefore there is a high variation in patterns and consequently the suggested system has the ability to discover new attacks. The new attack template rate measures the ratio of number new attack template that before we do not have this template to all attack traffic

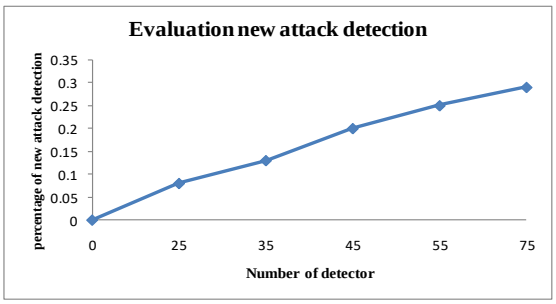


Fig.9. The percentage of new attack detection

5. CONCLUSION

Since establishing security in distribution networks is complicated to reach maximum security and detect portable attacks, it is important to use advantages of different methods of penetration detection. In a way that penetration detection in proposed system, use a combination of detection approach based on normal traffic and attack traffic. To analyze the proposed algorithm, we detain WiMAX message data by TCPDUMP tools. In each detection using genetic algorithm, a new generation is established that is added to antigen set, indeed, we detect new attack template that increases the ability of this system and by decreasing false positive, increased the accuracy of attack detection. The proposed system in this paper, after distinguishing the attack using policies minimize the attack influences and optimize the operation of system. In addition to that proposed system, collaboration between nodes and way of using artificial immune system algorithms is studied. In following papers, by using the operation of regulating T cells, normal nonself templates to decrease false negative. Also, by considering vaccine process in detection virus, it can be announced to detect system that there is an attack and needed reactions should be shown and make some detectors for detection. As in this study, WiMAX has been used but in WiMAX network, the second version is used in research and yet it is not used practically, and this version has so many parameters such as encryption with public key and Kerberos authentication algorithms, so we can obtain desirable results by using proposed algorithms in network.

REFERENCES

[1]D. Pareit, I. Moerman, P. Demester, The history of WiMAX: A complete survey of the evolution in certification and standardization for IEEE 802.16 and WiMAX, IEEE Communication, vol. 14, no. 4(2012): 1183–1211.

[2]Y. Zou, J. Zhu, X.Wang, L. Hanzo, A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, Vol. 104, No. 9, (2016): 1123-1161.

[3]P. Jadon, Detection and Mitigation of Flooding Attack in WIMAX Network, International Journal of Current Trends in Engineering & Technology, Volume: 02, Issue: 03(2016): 823-828.

[4]G.Oikonomou, P. Reiher, M. Robinson, and J. Mirkovic. "A framework for collaborative DDOS defense." *in Proceedings of the 2015 annual computer security applications conference*, (2015): 33-42.

[5]Ch. Zhang, Zh. Cai, W.Chen, X.Luo, J. Yin, Flow level detection and filtering of low-rate DDoS, Computer Networks 56 (2014) : 3417–3431.

[6]Daniel SIMION, M.-F. U.. An Overview on WiMAX Security Weaknesses/Potential Solutions. *11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania* , (2012): 110-117.

[7]M Alzaabi, K. D. SECURITY ALGORITHMS FOR WIMAX. *International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3* , (2013): 62-75.

[8]F. Esponda,S. Forrest and P. Helman. "A formal framework for positive and negative detection schemes." *IEEE Transactions on System, Man, and Cybernetics 34(1)*, (2014): 357–373.

[9]j. Balthrop, S. Forrest and M. Glickman. "Revisiting lisys: Parameters and normal behavior." *In CEC-2002: Proceedings of the Congress on Evolutionary Computing*, (2002).

[10] S. Stepney, R. Smith, J. Timmis, and A. Tyrrell. "Towards a conceptual framework for artificial immune systems." *In Proceeding of the 9rd International Conference on Artificial Immune Systems (ICARIS), LNCS 3239*, (2015): 53-64.

[11] P. Williams, K. Anchor, J. Bebo, G. Gunsch, and G. Lamont. "CDIS: Towards a computer immune system for detecting network intrusions." *In In RAID 2014, volume 2212*, (2014): 117–133.

[12] U. Aickelin, P. Bentley, S. Cayzer, J. Kim and J. McLeod. "Danger Theory: The Link between Artificial Immune Systems and Intrusion Detection Systems." *Proceedings 2nd International Conference on Artificial Immune Systems*,(2013): 147-155.

[13] P. Jadon, Detection and Mitigation of Flooding Attack in WIMAX Network, International Journal of Current Trends in Engineering & Technology, Volume: 02, Issue: 03(2016): 823-828.

[14] G.Oikonomou, P. Reiher, M. Robinson, and J. Mirkovic. "A framework for collaborative DDOS defense." *in Proceedings of the 2015 annual computer security applications conference*, (2015): 33-42.

[15] S. Singh. "Anomaly detection using negative selection based on the r-contiguous matching rule." *in Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS'-15)*, (2015): 99-106.

[16] W. Zhang, J. Lin, H. Jing, and Q. Zhang. " A Novel Hybrid Clonal Selection Algorithm with Combinatorial Recombination and Modified Hyper mutation Operators for Global Optimization", Computational Intelligence and Neuroscience Volume 2016, Article ID 6204728(2016): 1003-1016.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 185-192, 2018, ISSN:-2319–8656

Techniques to Control Memory Hogging by Web Browsers: An in-Depth Review

Harun K. Kamau
School of Computing and Informatics
Maseno University, Maseno, Kenya

Dr.O.McOyowo
School of Computing and Informatics
Maseno University, Maseno, Kenya

Dr.O.Okoyo
School of Computing and Informatics
Maseno University, Maseno, Kenya

Dr.C.Ratemo
School of Computing and Informatics
Maseno University, Maseno, Kenya

Abstract: The Web Browser is to date a popular piece of software in modern computing systems. They are the main interface for vast information access from the Internet. Browsers technologies have advanced to a stage where they do more than before. They now parse not only plaintext and Hypertext Markup Language (HTML), but also images, videos and other intricate protocols. These advancements have increased demand for memory. This increased demand poses a challenge in multiprogramming environments. The contemporary browser reference model does not have a memory control mechanism that can limit maximum memory a browser can use. This leads to hogging of memory by contemporary browsers. This paper is a review on emergent techniques that have been used to control memory hogging by browsers based on the contemporary reference architecture. We review major browsers architectures including Mozilla Firefox, Google Chrome and Internet explorer. We give an in-depth study on techniques that have been adopted with a view to solve this problem. From these reviews we derive the weaknesses of the contemporary browser architecture and inefficiency of each technique used.

Keywords: Browser reference architecture, memory hogging, web browser

1. INTRODUCTION

The Internet is progressively becoming an indispensable component of today's life. Most often than not, people largely rely on the expediency and elasticity of Internet-connected devices in learning, shopping, entertainment, communication and in broad-spectrum activities, that would otherwise necessitate their physical presence (Sagar A. et. al., 2010). Access to information or services via the Internet requires a medium; a browser operates as a medium. It is the prime component of a computer system when the Internet services are required. A browser retrieves, displays and traverses information resources on the web (World Wide Web Consortium, 2004).

Information resources comprise text, image, video, or other piece of content. These resources are accessed and indentified by a Uniform Resource Identifier (URI). The first browser known as WorldWideWeb was made in the early 1990s by Tim Berners-Lee (Tim Berners-Lee, 1999). Since then, browsers have seen tremendous advancements in their architectures and usage. The earliest browsers; Nexus, Mosaic and Netscape were less complex and used considerably low computer memory. However, they were commonly used for viewing basic HTML pages. With the birth of the Internet, browsers have gained a lot of popularity globally.

1.1 Motivation

Today, the browser is the most used computer application (Allan and Michael, 2006; Antero et. al., 2008). This phenomenon may be attributed to its various usages in everyday life. With limited computer power to process voluminous data generated from various sources, users have resorted to other technologies like the cloud computing and other online solutions where there is robust computer processing power, vast storage, scalability, reliability and on demand services. In these cases, resources are accessed as services via the Internet with thin clients especially the browsers.

Originally, Web information comprised a set of documents that in most cases contained text and hyperlinks to other related documents, having little or no client-side code. All rendered content originated from a single source. Web content has increasingly become more complex in pursuit to incorporate interactive features. Today, web programs have advanced to become highly interactive applications that execute on both the server side and client machine. With these advancements, modern web pages are no longer simple documents. They comprise highly dynamic contents that work together with each other. In other words, a Web page is now said to be a "system"– having dynamic contents as programs running in it, interacting

with users, accessing other contents both on the web page and in the hosting browser, invoking browser Application Programming Interfaces (APIs), and interacting with programs on the server side. These advancements require adequate computer memory in order to run properly from a host computer.

Consequently, these advancements in content rendering have raised memory demand browsers. In fact, memory allocation to a browser rises gradually from tens of Megabytes (Mbs), to hundreds of Mbs and eventually to Gigabytes (Doug DePerry, 2012). This fact only, categorizes browsers as today's memory "wolfs". Indeed, it leads to browser crash. The size of Random Access Memory (RAM) is an important factor in the running of software and consequently determines the level of multiprogramming. A single process consuming nearly a gigabyte of RAM in a one GB computer will lead to starvation of other processes and therefore lower multiprogramming level. This starvation may eventually lead to a crawl. However, these browsers behave differently in different platforms and with the content, the browser loads.

2. METHODS

The works reviewed were based contemporary browsers architecture and optimization techniques adopted thereon.

2. 1 Introduction

Today, browsers have advanced in terms of content rendering. This has raised memory demand for browsers. In fact, memory allocation to a browser rises gradually from tens of Megabytes (Mbs), to hundreds of Mbs and eventually to Gigabytes (Doug DePerry, 2012). This fact only categorizes browsers as today's memory wolfs. The size of RAM is an important factor in the running of software and consequently determines the level of multiprogramming; especially when it comes to browser efficiency. A single process consuming nearly a gigabyte of RAM in a one GB computer will lead to starvation of other processes and therefore lower multiprogramming level. This starvation may eventually lead to a crawl and even lead to the browser crashing. However, browsers behave differently in different platforms and with the content, they display.

2.2 Causes of Memory Hogging

Many users from the respective browser forums have regularly affirmed that memory hogging is attributed by several factors. To begin with is the length of the time the browser is used. As the browser gets used, gradually it will take more time to load during startup, the speed might decrease; and browsing eventually starts to slow down. This is a very frequent problem and occurs partially because of fragmentation in the databases browsers use. In particular, if Firefox is left running for a number of hours, consumed memory of well over a Gigabyte is observed even with only a few tabs open; a long running memory leak issue that plagues Firefox sometimes (Doug DePerry, 2012).

Secondly, when a user opens many tabs simultaneously, the browser will use more RAM. This is because each tab is designed to cache pictures, text and other active data, which keeps page data persistent while using multiple tabs. Expectedly, browsers such as Chrome and Firefox have ways to turn this behavior off, but the user may not wish it to happen. This is because, without caching, YouTube videos will not play in the background, and most real-time web apps will fail to work correctly.

Memory leakage is another factor. A memory leak happens when the browser for some reason doesn't release memory from objects which are not needed any more. This may happen because of browser bugs, browser extension problems and rarely, due to browser developer mistakes in the code architecture. Leaks may occur because of browser extensions, interacting with the page. More importantly, a leak may occur because of two extensions interaction bugs **(**Ilya Kantor, 2011). For instance, when Skype extension and the Antivirus are enabled, it leaks and when any of them is off, it doesn't.

2.3 Browser Reference Architecture

The following illustrates the convectional browser architecture adopted while building the contemporary browsers. We keenly look at how specific browsers have adopted this model.

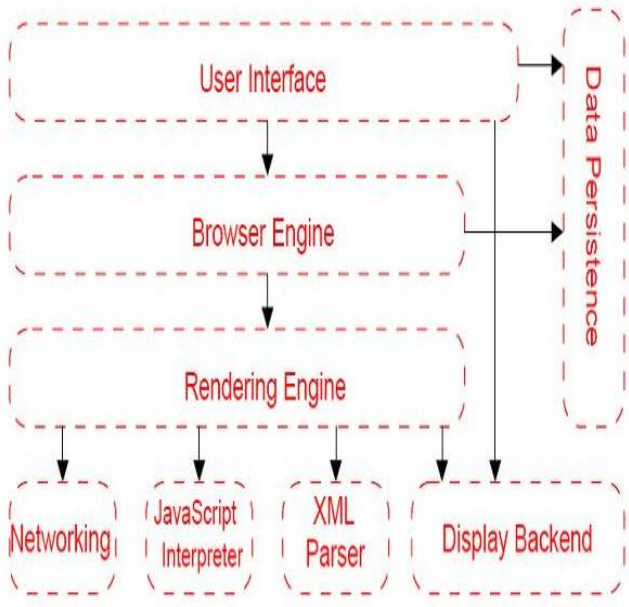


Figure 1: Browser Reference Architecture

The **User Interface** component provides the methods with which a user interacts with the Browser Engine. The User Interface provides standard features (preferences, printing, downloading, and toolbars) users expect when dealing with a desktop application.

The **Browser Engine** component provides a high-level interface to the Rendering Engine. The Browser Engine provides methods to initiate the loading of a Uniform Resource Locator (URL) and other high-level browsing actions (reload, back, forward). The Browser Engine also provides the User interface with various messages relating to error messages and loading progress.

The **Rendering Engine** component produces the visual representation of a given URL. The Rendering Engine interprets the HTML, Extensible Markup Language (XML), and JavaScript that comprises a given URL and generates the layout that is displayed in the User Interface. A key component of the Rendering Engine is the HTML parser, this HTML parser is quite complex because it allows the Rendering Engine to display poorly formed HTML pages.

The **Networking component** provides functionality to handle URLs retrieval using the common Internet protocols of Hypertext Transfer Protocol (HTTP), Hyper Text Transfer Protocol Secure (HTTPS) and File Transfer Protocol (FTP). The Networking components handle all aspects of Internet communication and security, character set translations and MIME type resolution. The Network component may implement a cache of retrieved documents to minimize network traffic.

The **JavaScript Interpreter** component executes the JavaScript code that is embedded in a website. Results of the execution are passed to the Rendering Engine for display. The Rendering Engine may disable various actions based on user defined properties.

The **XML Parser** component is used to parse XML documents.

The **Display Backend** component is tightly coupled with the host operating system. It provides primitive drawing and windowing methods that are host operating system dependent.

The **Data Persistence** component manages user data such as bookmarks and preferences.

3. BROWSER ARCHITECTURES

In a view to find how browsers have been developed, their architectures were reviewed to find out whether they are true derivations from the reference architecture.

3.1 Google Chrome

Google Chrome uses a multi-process architecture which gives it a competitive edge in performance over other browsers. Each tab has its own process which runs independently from other tabs. This allows one tab process to dedicate itself to a single web-application, thereby increasing browser performance. This protects the browser application from bugs and glitches in the rendering engine. Furthermore, it restricts access from each rendering engine process to others and to the rest of the system. This scenario offers memory protection and access control as manifested in operating systems. The multi-process architecture also increases the stability of the browser, as it provides insulation. In the case that one process encounters a bug and crashes, the browser itself and the other applications running concurrently are preserved.

Function wise, this is an improvement over other browsers, as highly valuable user information in other tabs will be preserved. Google Chrome has used the WebKit as a layout engine until version 27. Later versions have been using Blink.V8 has been used as JavaScript Interpreter in all versions. The components of Chrome are distributed under various open source licenses. Although Google developers have variant components in their architectural design, they have derived it from the reference architecture.

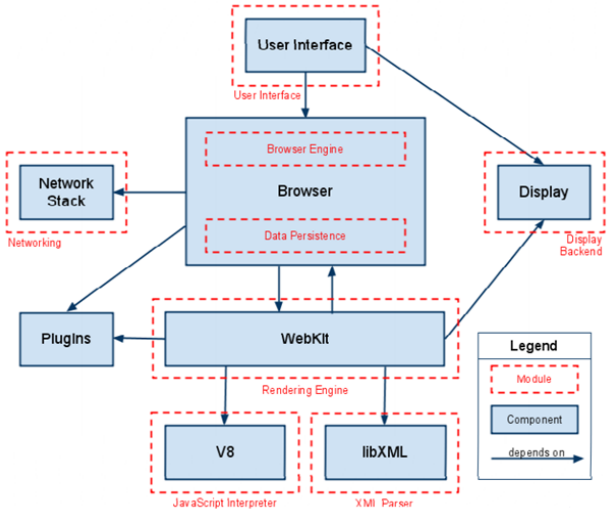


Figure 3.1: Google Chrome Architecture

3.2 Microsoft Internet Explorer

Essential to the browser's architecture is the use of the Component Object Model (COM), which governs the interaction of all of its components and enables component reuse and extensibility (MSDN, 2016). Internet Explorer uses Jscript and VBScript as JavaScript interpreter and Trident layout engine.

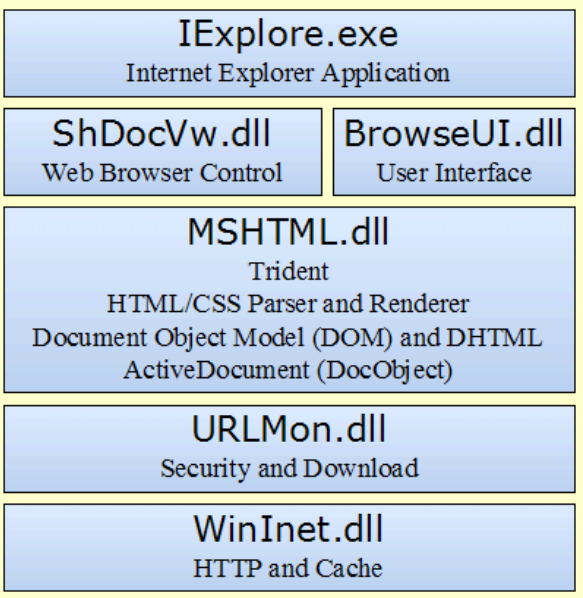


Figure 3.2: Internet Explorer Architecture

The following is a description of each of Microsoft Internet Explorer's six key framework components:

IExplore.exe is at the top level, and is the Internet Explorer executable. It is a small application that relies on the other main components of Internet Explorer to do the work of rendering, navigation, protocol implementation.

Browsui.dll provides the user interface to Internet Explorer. Often referred to as the "chrome," this Dynamic Link Library (DLL) includes the Internet Explorer address bar, status bar, menus, and so on.

Shdocvw.dll provides functionality such as navigation and history, and is commonly referred to as the WebBrowser control. This DLL exposes ActiveX Control interfaces, enabling you to easily host the DLL in a Windows application using frameworks such as Microsoft Visual Basic, Microsoft Foundation Classes (MFC), Active Template Library (ATL), or Microsoft .NET Windows Forms. When your application hosts 9999 the WebBrowser control, it obtains all the functionality of Internet Explorer except for the user interface provided by Browseui.dll. This means that you will need to provide your own implementations of toolbars and menus.

Mshtml.dll is at the heart of Internet Explorer and takes care of its HTML and Cascading Style Sheets (CSS) parsing and rendering functionality. Mshtml.dll is sometimes referred to by its code name, "Trident". Mshtml.dll exposes interfaces that enable you to host it as an active document. Other applications such as Microsoft Word, Microsoft Excel, Microsoft Visio, and many non-Microsoft applications also expose active document interfaces so they can be hosted by shdocvw.dll. For example, when a user browses from an HTML page to a Word document, mshtml.dll is swapped out for the DLL provided by Word, which then renders that document type. Mshtml.dll may be called upon to host other components depending on the HTML document's content, such as scripting engines (for example, Microsoft JScript or Microsoft Visual Basic Scripting Edition (VBScript)), ActiveX controls, XML data,

Urlmon.dll offers functionality for MIME handling and code download.

WinInet.dll is the Windows Internet Protocol handler. It implements the HTTP and File Transfer Protocol (FTP) protocols along with cache management.

Microsoft's Internet Explorer architecture utilizes the reference model components though variant in design.IExplorer.exe is a wrapper for the whole application. **Browsui.dll** serves as user interface while **Shdocvw.dll** performs functions of a browser engine**.** The **Mshtml.dll** is the core component that serves as rendering engine**.** It has HTML, CSS, XML and JavaScript parsers. **WinInet.dll** provides networking functions as provided for in the reference architecture.

3.3 Mozilla Firefox

The following model has been used in the design of Mozilla Firefox (Andre C. et al. 2007).

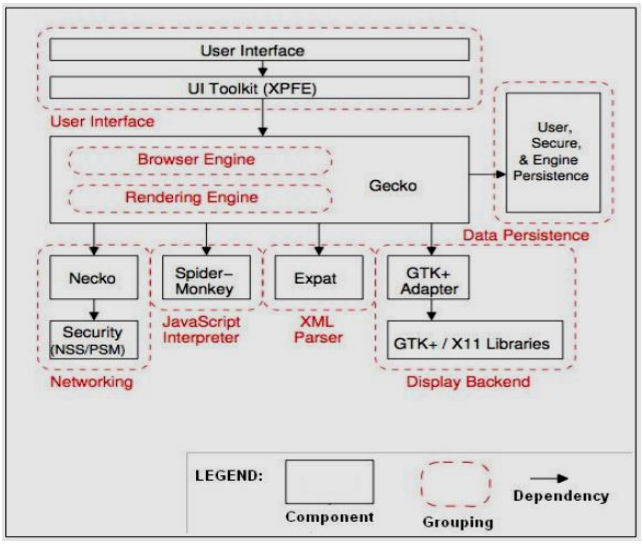


Figure 3.3: Mozilla Firefox architecture

The User Interface is split over two subsystems, allowing for parts of it to be reused in other applications in the Mozilla suite such as the mail/news client. All data persistence is provided by Mozilla's profile mechanism, which stores both high-level data such as bookmarks and low-level data such as a page cache.

Mozilla's Rendering Engine is larger and more complex than that of other browsers. One reason for this is Mozilla's excellent ability to parse and render malformed or broken HTML. Another reason is that the Rendering Engine also renders the application's cross-platform user interface. The User Interface (UI) is specified in platform-independent Extensible User Interface Language (XUL), which in turn is mapped onto platform-specific libraries using specially written adapter components. This architecture distinguishes Mozilla from other browsers in which the platform-specific display and widget libraries are used directly, and it minimizes the maintenance effort required to support multiple, diverse platforms.

Recently, the core of Mozilla has been transformed into a common runtime called XULRunner, exposing the Rendering Engine, Networking, JavaScript Interpreter, Display Backend, and Data Persistence subsystems to other applications. XULRunner allows developers to use modern web technologies to create rich client applications, as opposed to typical browser-based web applications. In fact, the Mozilla developers are working on transitioning newer Mozilla-based applications such as Firefox and Thunderbird to use XULRunner directly, rather than each using a separate copy of the core libraries. All components of this model fits exactly to those in the reference architecture.

3.4 Weaknesses of the Current Browser Architecture

a) The rendering engine processes the requests made by the browser engine by giving a visual display of the URL. This happens provided there is little memory available for use by the browser. If the operating system can no longer allocate any more memory, the computer freezes hence becomes unusable.

b) The browser process prevents other legitimate processes from being loaded in the main memory if it consumes almost all-available memory. This reduces the level of multiprogramming.

From the review of the above named architectures, memory hogging still remains a thorny issue. In attempt to reduce the its impact, third party software have been developed.

4. MEMORY OPTIMIZATION TECHNIQUES

To free memory that is unnecessary to the browser, several third party tools have been used. Memory optimization programs include but not limited to the following:

4.1 Firemin

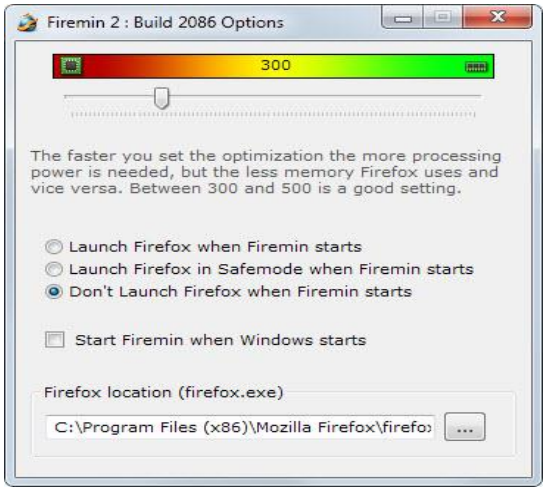
With Firemin for Firefox, you can effectively stop Firefox memory leaks automatically. As memory usage of this popular browser increases, your system slows down and you're stuck with limited system resources. In fact, Firefox can use up to 500MB of memory if you use the browser continuously (F. Ortega, 2013). Firemin forces Firefox to give back the memory it took from Windows and allows you to use Firefox in an optimized environment.

Firemin does not do anything that Windows does not do itself when the system runs out of RAM. It calls the Windows function EmptyWorkingSet over and over again in a loop to free up memory. Calling the function removes as many pages as possible from the working set of the specified process. The program ships with a slider that you can use to set the desired interval in which you want it to call the function.

However, the limitations of Firemin.exe are that, the technical security rating is 30% dangerous. This is because it records keyboard and mouse inputs, monitors applications and manipulates other programs. Moreover, some malware

camouflages itself as Firemin.exe, particularly when located in the C:\windows or C:\windows\System32 folder. Also, Firemin is only compatible with Mozilla Firefox.

Figure 4.1: Firemin



4.2 Wise Memory Optimizer

Wise Memory Optimizer helps you free up and tune up the physical memory taken up by some unknown non-beneficial applications to enhance PC performance. You can enable automatic optimization mode when the free PC memory goes below a value that you can specify, and make Wise Memory Optimizer run even when the CPU is idle, as well as adjust the amount of memory you want to free up. Then it will optimize PC memory automatically in the background.

However, this tool does not prevent the browser from hogging memory it only reclaims memory from unknown non-beneficial applications.

Figure 4.2: Wise memory optimizer

4.3 SpeedyFox

SpeedyFox is a tool designed specifically for compacting the SQLite database files which will in turn reduce the time taken to read from and write to them. In addition to Firefox which it was originally designed for, SpeedyFox can now also compact the databases for the Chrome, Epic Browser, SRWare Iron and Pale Moon browsers. It also supports the Mozilla Thunderbird and Skype tools as well.

Upon running the portable executable, SpeedyFox automatically detects and loads the default profile for each of the supported applications. As they're very popular these days, it's also possible to load custom profiles for Firefox or Chrome portable versions. Click the SpeedyFox menu bar and select "Add custom profile" or drag the profile folder and drop it onto the SpeedyFox window.

Simply tick the application profiles to optimize and click the Optimize! Button, SpeedyFox will start to compact the SQLite databases. The progress window shows what databases are optimized and also how much space is saved. You need to make sure the programs being optimized are not running at the time or they won't be processed. In a quick test it reduced 14MB of Firefox databases to 6MB and 192Mb of Chrome databases to 186MB. The author of SpeedyFox recommends running the tool every 1-2 weeks depending on your usage of the included browsers.

Though tool increases Mozilla Firefox launch speed, it does not prevent memory hogging. It just clears cache over some time.

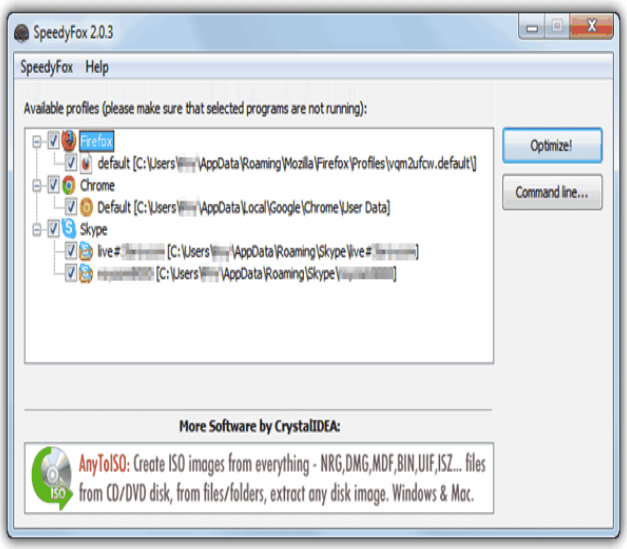


Figure 4.3: SpeedyFox

4.4 All Browsers Memory Zip

All Browsers Memory Zip has no database compacting functions but is a dedicated memory-optimizing tool for a large number of popular web browsers. It works very much like another memory optimizer called CleanMem, but this tool only handles browsers. In addition to Chrome and Firefox, it also works with other popular browsers like Opera, Internet

Explorer and Maxthon etc. The program is portable but has separate 32-bit and 64-bit versions, and when you run it there will be a small tooltip and then All Browsers Memory Zip will sit in the system tray optimizing the memory of any running supported browsers. If you open Task Manager (Ctrl+Shift+Esc) before you launch the tool, you will see the used memory for the browser process suddenly decreases by a massive amount. It is not uncommon to see 1GB+ in memory usage drop to fewer than 10MB in a few seconds.

Right click on the tray icon to pause the program from optimizing and pressing Usage Controller will popup the window above that will allow you to set the maximum amount or RAM for each browser and edit the shortcut keys. Just select the browser form the dropdown, enter the max amount in Megabytes and click Set.

This tool must execute all times a browser process is running. It requires a significant amount of memory. Consequently, it impacts negatively when streaming content over the Internet.

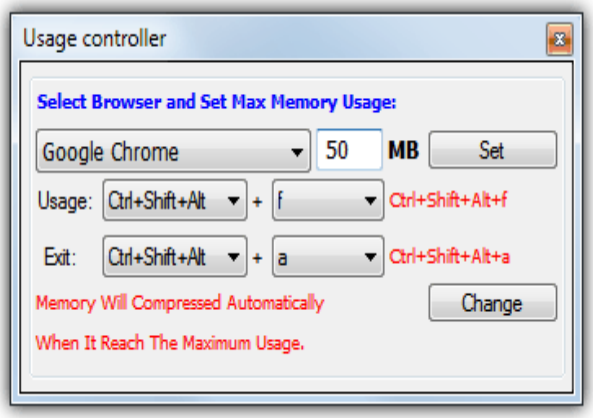


Figure 4.4: All browsers zip usage controller

5. CONCLUSION

A review on various techniques adopted in a view to control memory hogging was presented in this paper. It is evident enough that memory hogging among various browsers is and still a thorny issue. It is desired that computer applications use little memory and execute faster with a view to allow as many programs to be loaded in the main memory for execution. With browsers being among such applications, this still remains an issue under investigation. Many third party applications have been developed in quest to reduce memory consumption. These applications include Firemin, Wise Memory Optimizer, SpeedyFox and All browsers memory zip. After all these tools have been analyzed, it has been found out that, memory control is not efficient, poor compatibility issues, overhead to users and decrease in browser performance. An interesting issue has been found on the browser reference architecture. The contemporary architecture in use today aggravates this problem. It has been found out that, this model lacks memory control mechanism which would complement these third party applications. Today, browsers have become a major platform through which resources accessed via the Internet are availed to the user. Based on this fact, memory as prime resource has remained a major limitation while trying to run applications through the browser. This has become a major drawback in multi programming environment. A new approach to incorporate a memory analyzer in the architecture has been suggested. It is hoped that this shall control memory hogging and reduce overhead to the browser application while optimizing memory.

6. REFERENCES:

[1] A. E. Hassan and R. C. Holt, (2000). A reference architecture for web servers. In Proceedings of 7th the Working Conference on Reverse Engineering (WCRE ’00), pp. 150–160, 2000.

[2] A. Mockus, R. T. Fielding, and J. Herbsleb, (2002) Two case studies of open source software development: Apache and Mozilla. In ACM Trans. Software Engineering and Methodology, pp. 11(3), 309–346, 2002.

[3] A. Taivalsaari and T. Mikkonen, (2011). "The Web as an Application Platform: The Saga Continues," *Proc. 37th Euromicro Conf. Software Engineering and Advanced Applications* (SEAA 11), IEEE CS, 2011, pp. 170–174.

[4] A. Taivalsaari et al., (2008). Web Browser as an Application Platform: The Lively Kernel Experience, tech. report TR-2008-175, Sun Microsystems Labs, 2008.

[5] Accuvant Labs, 2011: Browser Security Comparison; A Quantitative Approach. Retrieved from http://files.accuvant.com/web/files/AccuvantBrowserSecCompar_FINAL.pdf

[6] Adam Overa, 2011: Web Browser Grand Prix 3: IE9 Enters The Race. Efficiency Benchmarks: Memory Usage and Management. Retrieved from http://www.tomshardware.com/reviews/internet-explorer-9-chrome-10-opera-11,2897-11.html

[7] Adèr, H.J. & Mellenbergh, G.J. (2008). *Advising on Research Methods: A consultant’s companion.* Huizen, the Netherlands: Johannes van Kessel Publish.

[8] Ahmed E. Hassan, Michael W. Godfrey, and Richard C. Holt, n.d. Software Engineering Research in the Bazaar.

[9] Alan Grosskurth and Michael W. Godfrey, (2005) Reference architecture for web browsers. In ICSM'05: Proceedings of the 21st IEEE International Conference on

Software Maintenance (ICSM'05), pp 661-664, Washington, DC, USA, 2005. IEEE Computer Society.

[10] Alan Grosskurth, Michael W. Godfrey ,(2006) Architecture and evolution of the modern web browser. Retrieved from http://grosskurth.ca/papers/browser-archevol-20060619.pdf

[11] Allan Grosskurth and Michael Godfrey, (2014). Reference architecture for web browsers. In Journal of Software Maintenance and Evolution: Research and Practice, pp 1–7, 2006

[12] Avant Force, (2016). Retrieved from http://www.maxthon.com/about-us/

[13] Chris Anderson (2012). The Man Who Makes the Future: Wired Icon Marc Andreessen. Retrieved from http: //www.wired.com/2012/04/ff_andreessen/all/

[14] Doug Deperry, (2012). HTML5 security in the modern web browser perspective**.**

[15] Gnome desktop environment. Home Page. Retrieved from Http: //gnome.org.

[16] Karl Gephart (2013): Optimize Firefox's Performance with these Memory Add-Ons! : Retrieved from http://www.drakeintelgroup.com/2013/06/25/Firefox-memory-addons/

[17] Krause, Ralph (March 2000). Browser Comparison. Retrieved from http://www.linuxjournal.com/article/5413

[18] Matthew Braga (2011): Web Browser Showdown: Memory Management Tested. Retrieved from http: //www.tested.com/tech/web/2420-web-browser-showdown-memory-management-tested/index.php

[19] Maxthon International Ltd, (2014). Retrieved from http://www.maxthon.com/about-us/

[20] Nick Veitch, (August 2010). 8 of the best web browsers for Linux. Retrieved from http://www.techradar.com/news/software/applications/8-of-the-best-web-browsers-for-linux-706580/3

[21] Nyce, J. M. & Kahn P., (1991).From Memex To Hypertext: Vannevar Bush and the Mind's Machine. Academia press, San Diego.

[22] Opera Software, (February, 2003). "Opera version history". Retrieved from http://www.opera.com/docs/

[23] Pour, Andreas (January, 2003). "Apple Announces New "Safari" Browser". KDE Dot News. Retrieved from https://dot.kde.org/2003/01/08/apple-announces-new-safari-browser

[24] Sagar, A., Pratik, G., Rajwin, P. and Aditya, G., (2010). Market research on web browsers. Retrieved from http://www.slideshare.net/sagar_agrawal/research-on-web-browsers.

[25] T. Mikkonen and A. Taivalsaari, (2007) "Web Applications – Spaghetti Code for the 21 Century". Retrieved from http://research.sun.com/techrep/2007/abstract-166.html (presented in the SERA Conference, Prague, Czech Republic, August 21, 2008)

[26] T. Mikkonen and A. Taivalsaari, (2008) "Web Browser as an Application Platform: The Lively Kernel Experience" http://research.sun.com/techrep/2008/abstract-175.html (presented in the SEAA Conference, Parma, Italy, September 4, 2008)

[27] T. Mikkonen and A. Taivalsaari, (2011). "Apps vs. Open Web: The Battle of the Decade," *Proc. 2nd Workshop Software Eng. for Mobile Application Development* (MSE 11), 2011; Retrieved from http://www.mobileseworkshop.org/papers6-Mikkonen_Taivalsaari.pdf.

[28] Tim Berners-Lee (1999). Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor. Harper San Francisco.

[29] W3C (2004). Architecture of the World Wide Web, Volume One. Online. Retrieved from http://www.w3.org/TR/webarch/

[30] Wayner, Peter (January, 2005). "BASICS; Custom Tailor A Web Browser Just for You", The New York Times, ISSN 0362-4331, OCLC 1645522. Retrieved from http://query.nytimes.com/gst/fullpage.html?res=9C0DE6D9163BF934A15752C0A9639C8B63