Challenges and Issues of E-Learning Using Education Cloud – A Review in Context of Covid-19 Pandemic

Saifallah Al Kati
College of Computer Science and Information Science
Imam University
Riyadh, Saudi Arabia

Muhammad Asif Khan
College of Computer Science and Engineering
Taibah University
Madinah, Saudi Arabia

Abstract: During the recent Coronavirus (Covid-19) pandemic the traditional education system almost halted throughout the world. However, in order to continue with the education without wasting students time most of the countries transferred their teaching online. Although the online teaching is widely used but there are many challenges and security issues specially when the education is disseminated using education cloud. In this article we examine and review such challenges and security issues that may impact students and teachers in various educational institutions in Saudi Arabia. A review of hybrid cloud model is presented in order to benefit across institutions. The research also articulates different ways which can be adopted by educational institutions to provide smooth online teaching due to pandemic of covid-19. We also present some solutions that may help overcome challenges and secure a robust cloud infrastructure.

Keywords: cloud computing; e-learning; issues; challenges; online teaching; covid-19

1. INTRODUCTION

A respiratory disease due to Coronavirus (Covid-19) originated from bats in China in late 2019 [1]. The virus spread out throughout the world very rapidly. Businesses, industries, educational institutions and recreational activities were shut down in order to prevent pandemic from spreading at large scale. All researchers and practitioners agreed that social distancing is the only cure to protect from pandemic and this is why people were advised to maintain a distance from interacting each other. All gaits of life were affected and education is one of them where student-teacher interaction was inevitable. Therefore, educational institutions were shut down in compliance with social distancing rule. Various institution adopted e-learning strategy in order to continuously providing teaching to students. In Saudi Arabia enormous precautionary measures were taken in all areas in order to prevent from virus spread across the country. The ministry of education suspended in-person teaching activities in all public and private educational institutions and instructed to continue teaching online without delay of even one day [2].

In order to provide a seamless teaching to students online and assessing them though various assessments methods, resources should be available all the time. Since each institution is responsible to ensure resources are in place in institutional servers it becomes more complex, expensive and hectic. The best solution is to use a cloud computing where all teaching and assessment materials are available with convenience and ease.

1.1 Cloud computing

A cloud is a group of servers that are available on internet and provide different functionality to various clients. Servers have different types such as application server, database server, web server etc. Cloud computing refers to availability of computing and storage resources i.e. servers over internet. These resources are available to many users over internet at a time without compromising of data loss and data security. Cloud computing helps organizations to prevent infrastructure costs and still can use desired applications and manage data with minimum cost without any hassle. Servers are available in data centers, which enable users to access their data and applications without maintaining and updating them. Cloud computing is more useful for small businesses where technology infrastructure is more expensive than outsourcing the required resources.

1.2 Cloud services

There are different cloud computing service models that are available to users by different cloud service providers. [3] described three service models that are common in industry i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

1.2.1 Cloud services

A cloud service provider offers virtual data storage and servers to users who may develop their own applications using the resources available in the cloud. In this service model operating systems, data storages and various applications are maintained by cloud service providers. A business client may choose the services as per requirements and pay the prescribed charges based on the usage of the services. This model is scalable which does not require any installation on premises and reduces cost. Figure 1A shows this model.

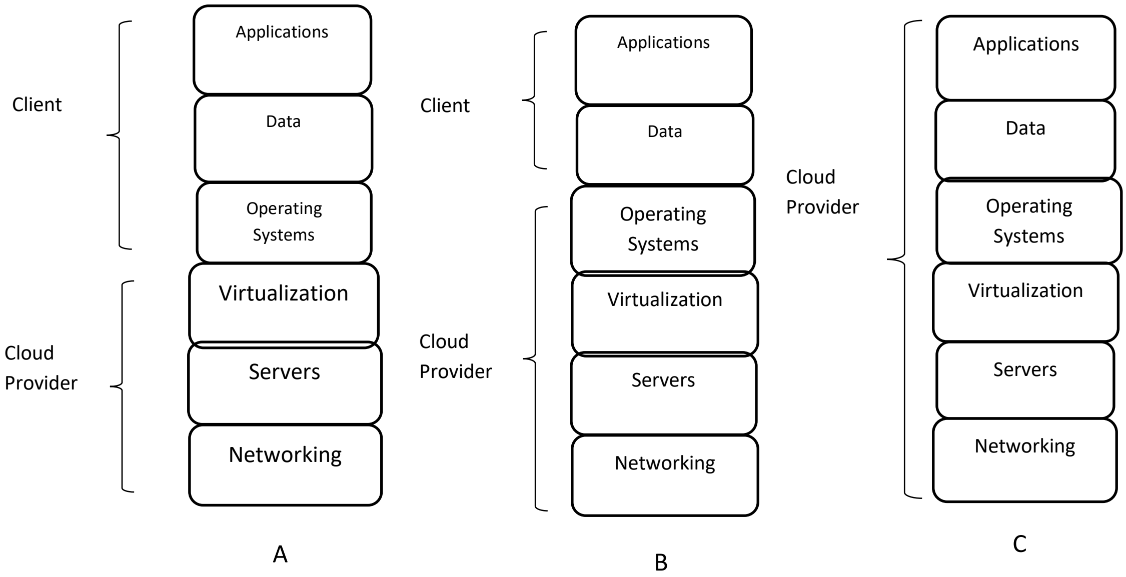


Figure 1. Cloud services infrastructure

1.2.2 Platform as a Service (PaaS)

This model provides users with a platform to develop, manage and test their applications that abridges the development process. The cloud provider provides servers, storage and network resources to users for developing applications and manage them by either users or the service provider. Figure 1B depicts the PaaS model.

1.2.4 Software as a Service (SaaS)

In this service model, cloud service provider hosts software applications and facilitates users to access the software on demand through internet. Users may develop their own business application using the software and either save data locally or in the cloud. In this, users always find updated software and its functionalities without any hassle of availability of new version of the software. Figure 1C shows this model.

In order to deploy cloud services there are mainly three types of cloud i.e. public cloud, private cloud and hybrid cloud.

Public cloud allows users to use the infrastructure provided by a cloud service provider. The cloud infrastructure is established and maintained at the premises of cloud service provider and thus users do not have any control on that. Various clients share the resources which, in turn reduces cost, but the security may be compromised and vulnerability exists. In private cloud infrastructure is dedicated to one company or user without any sharing of resources. In this type of cloud security is high, but if clients requires infrastructure can be provided to the client's premises for more security and control of the resources. A hybrid cloud is composed of public and private clouds. It is usually used by those companies which give access of products to their customers and interact with them through public cloud whereas the company maintains private data in a private cloud.

1.3 Research Question

In this research we strive to answer the following research question:

What are security challenges and issues of cloud computing that hamper online higher education in Saudi Arabia.

1.3.1 Research Motivation

Cloud computing services have been adopted throughout the globe due to their usefulness and economic feasibility. In order to fulfil educational institutions education cloud has been in use by different organizations and various educational tools and services are provided by the cloud service providers. In Saudi Arabia many universities are using education cloud to provided optimum teaching and learning facilities. However, there have been several issues and challenges which universities experience around the world. Due to such issues educational institutions face difficulties to provide required level of quality education. We aspired to find challenges and issues that universities in Saudi Arabia face and need to resolve them in order to continue providing quality education online.

2. LITERATURE REVIEW

Cloud computing paradigm facilitates sharing of pool of resources and its scalability feature convinces businesses to adopt this paradigm at low cost. Rapid increase in adoption of latest technology has encouraged educational institutions of higher learning to use cloud computing in order to develop global interaction, communication and cooperation [4]. In the prevailing situation due to Covid-19 pandemic educational institutions are planning to transform formal education to online education or e-learning. It is imperative for educational establishments to concentrate on imparting effective education and learning instead of focussing on technology infrastructure. Cloud computing paradigm ensures that educational institutions focus on education and effective delivery of contents to students without developing and installing software and applications [5]. In order to communicate and collaborate with other educational institutions it is necessary to have a common place where organizations could share their resources such as course material, assessments, projects etc. A hybrid cloud computing model was presented by [6] for higher educational institutions in Saudi Arabia in which such sharing of resources proposed. E-learning was adopted in

Saudi Arabia somewhat is 1990s, but a sharp rise happened due to growth in technology and internet [27]. Saudi government set up an IT plan to induct technologies at all levels especially higher education and established distance learning centers [28]. Universities in Saudi Arabia have been active in e-learning such as King Abdulaziz University, King Fahad University of Minerals and Petroleum, Taibah University, King Saud University, King Faisal University, Qassim University etc.

In view of recent Covid-19 pandemic spread, the ministry of education Saudi Arabia suspended all formal teaching in public and private institutions beginning from March 8, 2020 until further notice [7]. However, the ministry immediately launched e-learning through learning management system in order to continue studies without disruption and to save students time. The e-learning provides convenience to both students and faculty in terms of place, time and learning resources. Due to its convenience, e-learning is being adopted throughout the globe and it is replacing the traditional teaching system [8]. Faculty members can share and update the same teaching material and deliver it with confidence to their students.

However, researchers have identified some challenges in implementation of e-learning such as scalability and infrastructure that need to be updated and configured with the growth of workloads [9]. In a study conducted for Kenyan Higher Education this has been reported that in success of e-learning, apart of computing technology, quality and character of an institution plays a significant role [10]. Although initially e-learning was considered as a mean of convenience, collaboration, cost effectiveness, scalability and availability, but now it is an essential continuous source of education for students in view of covid19 pandemic. In turn, cloud computing services are gaining popularity and many challenges are also increasing accordingly. In a study [11] some challenges such as data privacy and cloud infection were reported. Some other challenges like technology awareness, infrastructure, culture, instructor competency and readiness from students and faculty were discussed in developing countries [8]. The increasing growth in technology has fascinated the Generation Y who is e-learning prone due to its convenience and availability [12] and therefore, it seems despite of various challenges and issues e-learning will become an effective and popular mode of study among the large population of students [13]. Some challenges and security issues in cloud have been reported such as surveillance of virtual machine from a host or another virtual machine, data access by malicious program, inadequate provisions in service legal agreement (SLA) and failure in complying standards [14][15][16].

In order to meet the demands of e-learning in Saudi Arabia, the ministry education, Saudi Arabia has established a national e-learning center (NeLC) with the aim to provide quality education. The center provides licenses to the entities which provide e-learning education as per standards defined by the NeLC [17]. In a study [18] various issues and concerns were examined in adoption of cloud computing in public sector. In view of increasing demands of cloud computing services are being provided in educational institutions. In another study [19], the growing trend of e-learning in Saudi Arabia is highlighted and various factors such as support, training, incentives to faculty for e-learning growth have been mentioned. Many prominent cloud service providers such as Microsoft, Google and IBM are providing attractive programs for education such as GoogleDocs, Google Drive, Office 365 and IBM Academy [20].

3. MATERIAL AND METHODS

In order to determine the trend in e-learning security challenges in issues in education cloud, qualitative methodology is appropriate which provides a set of different methods for deep insight. We collected qualitative data from various articles, interview meetings and reports, in order to analyze the issues and challenges in e-learning through education cloud. Since our focus is Saudi Arabia, we collected relevant data using different methods stated above.

Qualitative methods are flexible and provide opportunity to design and improve system in view of people’s experiences and perceptions. Qualitative research helps to unfold findings in natural setting without manipulating natural phenomenon [21]. The data collected by these methods is from real world and can be adapted to explore new opportunities. Case studies provide data that is generated in real time and can be verified. Case studies use face on face interviews, focus groups and survey instruments for collecting first hand data from various sources. In our study we used case studies, which use cloud technology especially education cloud for e-learning. The case studies help to determine various issues and challenges that educational institutions face during online teaching especially in Saudi Arabia. The data collected from literature provided us foundation to investigate the issues and challenges in Saudi educational institutions. In order to collect data investigated higher educational institutions that use educational cloud. We selected five major public higher educational organizations in Saudi Arabia which agreed to provide data on anonymous condition. We contacted the responsible persons of respective departments in the institutions in order to collect data on various issues and challenges. For this purpose, we held face-to-face meetings and collected first hand data. Also, we uploaded a questionnaire on a website and received 109 responses from all the five institutions, out of which 98 found to be complete and trustworthy. In order to measure reliability, the internal consistency in responses was checked and standard general test Cronbach’s Alpha was conducted that resulted in 0.67 value. The Cronbach’s alpha value shows the reliability of the responses we received. Table 1 shows some sample of questions that were asked in the questionnaire on Likert’s scale.

Table – 1. Sample questions from questionnaire

No.	Question phrase
1	We consider our resources including teaching material secure online
2	Our students did not experience difficulties due to immediate shift online during Covid-19 pandemic
3	We have enough knowledge of technological infrastructure to support e-learning
4	Our online system is robust and cloud services never failed during teaching
5	We are satisfied with the performance of cloud services and e-learning
6	Students were comfortable during online assessments and no issues raised

7	Instructors experienced difficulties in preparing online assessments
8	Cloud services provided all necessary tools required for preparing online assessments
9	Our cloud service provider support has been available whenever we needed
10	Our students cooperated in online learning and evaluation caused by pandemic covid 19

The severity or significance of security issue in organizations was determined through the data collected by interviews and questionnaire. We used Likert's scale 1-5in order to determine significance in which, 5 means very high and 1 indicates very low significance of the issue or challenge.

4. RESULTS AND DISCUSSION

We collected data through various literature, interviews, documents, questionnaire in order to find out the difficulties, challenges and issues in public education institutions in Saudi Arabia. The institutions used the cloud computing services and provided information about their experience.

Table 2 shows the number of respondents for the significance of the issues and challenges in the public educational organizations (mentioned as A through E for privacy) in Saudi Arabia. These issues and challenges have been extracted from the literature as well as question phrases in questionnaire that were reconfirmed by the respondents.

Table – 2. Number of respondents for significance of issue/challenge

Issue/Challenge	**Literature/ Reference**	**Significance**					**Mean**	**Standard Deviation**
		Very high	**High**	**Neutral**	**Low**	**Very low**		
Privacy	[11][18][21]	45	38	3	8	4	4.1428	0.54300
Data security, risk	[21]	36	39	2	13	8	3.8367	0.49734
Infrastructure	[8]	38	41	4	7	7	3.9489	0.51536
Quality of education	[24][25]	43	44	1	8	2	4.2040	0.56982
Culture and training	[25]	28	32	8	12	18	3.4081	0.42443
Cloud control	[26]	41	38	4	8	6	3.9897	0.51493
Performance	[26]	39	41	3	10	5	4.0102	0.52334

As we can see from the above figure 1 the majority of the respondents considered quality of education as most significance issue. Usually, in Saudi Arabia government strives to provide quality education to its citizens and technology infrastructure has been developed swiftly throughout the kingdom. Similarly, privacy is another major issue for educational organizations so that educational data and students information are protected while learning online. Performance of online education has been important to the institutions and from the fig. 1 it appears that respondents gave importance to the performance whereas cloud services were also important.

We conclude from the data that our research question has been answered by identifying the issues like quality of education, privacy, performance and cloud control that have to be addressed continuously in order to provide seamless online education.

We also determined that overall public institutions were satisfied with the infrastructure and cloud services provided by service providers for online teaching due to Covid19 pandemic. However, there are some concerns for online assessments that need to be addressed in future.

5. REFERENCES

[1]. Wu, F., Zhao, S., Yu, B., Chen, Y.-M., Wang, W., Song, Z.-G., et al., (2020) “A new coronavirus associated with human respiratory disease in China” *Nature*, No. 575, pp. 265-269

[2]. www.spa.gov.sa/2050320 , Saudi Press Agency, [Accessed on July 16, 2020]

[3]. Lee, K, (2012) “Security threats in cloud computing environments”, *International journal of security and its applications*, No. 6, 25

[4]. Shahzad, A., Golamdin, A., Ismail, N., (2016) “Opportunity and Challenges using the Cloud Computing in the Case of Malaysian Higher Education Institutions”, *The International Journal of Management Science and Information Technology*, 20, pp. 1-18

[5]. Alberto, F., Daniel, P., José, B., and Francisco, H., (2012) “An Overview of E-Learning in Cloud Computing”, *Advances in Intelligent Systems and Computing*, No. 173. 10.1007/978-3-642-30859-8_4

[6]. Khan, M. A., (2016) "A Hybrid Cloud Model for Higher Education Institutions in Saudi Arabia", *6th International Conference on Cloud Computing (CLOUDCOMP2015), LNICST*, No. 167, pp. 255-259

[7]. https://www.moe.gov.sa/en/HigherEducation, Guide to exams and evaluation arrangements Covid-19 [Accessed on July 27, 2020]

[8]. Yang, H. H., Feng, L., & MacLeod, J. (2019) “Understanding College Students’ Acceptance of Cloud Classrooms in Flipped Instruction: Integrating UTAUT and Connected Classroom Climate”, *Journal of Educational Computing Research*, No. 56, pp. 1258–1276

[9]. Fern´andez, A., D. Peralta, D., Herrera, F., and Ben´ıtez, J., (2012) “An Overview of E-Learning in Cloud Computing”, *L. Uden et al. (Eds.):Workshop on LTEC 2012, AISC*, No. 173, pp. 35–46

[10]. Islam, N., Beer, M., and Slack, F., (2012) “E-Learning Challenges Faced by Academics in Higher Education: A Literature Review”, *Journal of Education and Training Studies*, No. 3, pp. 102-112

[11]. Deepa, N., and Sathiyaseelan, R., (2012) “The Cloud and the Changing Shape of Education – Eaas (Education as a Service)”, *International Journal of Computer Applications*, No. 42, pp. 4-8

[12]. Markert, J, (2004) “Demographics of age: Generational and cohort confusion”, *Journal of Current Issues and Research in Advertising*, No. 26, pp. 11–25

[13]. Tagoe, M, (2012) “Students’ perceptions on incorporating e-learning into teaching and learning at the University of Ghana”, *International Journal of Education and Development Using Information and Communication Technology*, No. 1, pp. 91–103

[14]. Aldossary, S., and Allen, W., (2016) “Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions”, *International Journal of Advanced Computer Science and Applications (IJACSA)*, No. 7, pp. 485-498

[15]. Pushpa R., and Swapna K., (2012) “Issues & Solution of SAAS Model in Cloud Computing” ,*IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 40-44

[16]. Jiale Z., Bing C., Yanchao Z., Xiang C., and Feng H., (2018) “Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues” , *IEEE Access*, No. 6, pp. 18209-18237

[17]. National e-learning center [www.nelc.gov.sa/en] Accessed on Sep 15, 2020

[18]. Majid, A., Elhadj, B., and Khawar, H., (2018) “Key Issues for Embracing the Cloud Computing to Adopt a Digital ransformation: A study of Saudi Public Sector”, *Procedia Computer Science*, No. 130, pp. 1037–1043

[19]. Alshwaier, A., Youssef, A., and Emam, A., (2012) “A New Trend for E-Learning in KSA Using Educational Clouds”, *Advanced Computing: An International Journal*, No. 3, pp. 81-97

[20]. Sultan, N., (2010) “Cloud computing for education: A new dawn?”, *International Journal of Information Management*, No. 30, pp. 109-116

[21]. Patton, M., (2002) “Qualitative evaluation and research methods (3rd ed.)”, Sage Publications, Inc.

[22]. Juma, M.K., and Tjahyanto, A., (2019) “Challenges of Cloud Computing Adoption Model for Higher Education in Zanzibar (the case study of suza and zu)”, *Procedia Computer Science*, No.161, pp. 1046-1054

[23]. Mary, A. C., and Rose, A. L., (2019) “Implications, Risks and Challenges of Cloud Computing in Academic Field”, *International Journal of Scientific and Technology Research*, No. 8, pp. 3268-3278

[24]. Aljaber, A. (2018) “E-learning policy in Saudi Arabia: challenges and successes”, *Research in Comparative and International Education*, No. 13, pp. 176-194

[25]. Islam, N., Beer, M., and Slack, F., (2015) “E-Learning Challenges Faced by Academics in Higher Education: A Literature Review”, *Journal of Education and Training Studies*, No. 3, pp. 47-53

[26]. Edeh, M. O., Nwafor, C. E., Ugwugbo, A. N., Rockson, K. A., Ogbonnaya, U. N., (2020) “Cloud Security Challenge: Implication on Education”, *International Journal of Computer Science and Mobile Computing*, No. 9, pp.56-73

[27]. Al-Masaud, K., and Gawad, A., (2014) “Impediments of activating e-learning in higher education institutions in Saudi Arabia”,. *International Journal of Advanced Computer Science and Applications*, No. 5, pp. 12-18

[28]. Al-Asmar, A., and Khan, M. (2014) “E-learning in Saudi Arabia: Past, present and future”. *Near and Middle Eastern Journal of Research in Education* , No. 1, pp. 82-95

Smart Stadium using Cloud Computing and Internet of Things (IoT): Existing and New Models

Mustafa Jamal Mahdi
College of Engineering
Al-Iraqia University
Baghdad, Iraq

Abbas Fadhil Aljuboori
College of Engineering
University of Information Technology and Communications
Baghdad, Iraq

Mudhafar Hussein Ali
College of Engineering
Al-Iraqia University
Baghdad, Iraq

Abstract: In our life technology is important there are two entirely various technologies are cloud computing and the IoT and both are very portion of our lives. They are supposed to be more common in their acceptance and use, making them essential ingredients of the future Internet worldwide. Because of the lack of time in our working life and the follow-up of all operations that we must follow before any match is held on any stadium in the world. An aspect of precautionary measures is discussed here before every match. In this research, a discussion was conducted on how to integrate cloud computing and the IoT and use them to work in developing stadiums in the word and made it smart. Several existing and new models of smart stadium are although explained.

Keywords: IoT, Cloud Computing, Smart Stadium, Web Application, Smart Application.

1. INTRODUCTION

Smart Stadium for Smart Living is an effort intended to integrate IoT and smart stadium technology for organizations and partners. The initiative joins Arizona State University in Tempe- Arizona: Dublin City University in Dublin- Ireland: Gaelic Athletic Association of Ireland; and Intel Corporation to turn two stadia ASUs Sun Devil Stadium and Ireland's Croke Park Stadium into twinned smart stadia with the possibility to be world kind testbeds for exploring smart stadium apps and IoT solutions. To date, these initiatives have concentrated on two wide areas of implementation. 1- Enriching the fan/attendee trial, and 2- Improving operations at the stadium. While the implementation focus of these initiatives is set in the framework of events related to stadiums, they are applicable to broader areas of application for smart cities. Under these projects, the complete spectrum of projects covers crowd control, fan participation, event planning, by ply use a set of sensors like video cameras and mounted microphones, stadium security and environmental for monitoring issues [1]. Smart Stadium is an increasingly popular fact in cities across the world. The concept of a smart stadium is not recent, but it has changed largely due to the advent of new technologies, while implemented, allows smarter resources and processes to extend the stadium's ability to function in a more effective, scalable, interactive, and sustainable manner [1]. Football is one of the world's most common sports, which is why all suitable conditions for growth and advancement must be given. And in terms of setting rules, designing, and improving this game in all respects, the party responsible for this is FIFA. Many advancements that have changed the game have recently been implemented by the company responsible for the growth and advancement of the standard of football worldwide. For instance, Goal Line Technology (GLT) has been implemented to decide if the entire ball has reached the goal line to help referees make their decisions. [2][3]. Furthermore, to build safe and comfortable environments, FIFA has issued technical guidelines and criteria for the construction of new football stadiums [4]. Of requirements and things organized a special football pitch should note that several aspects including lighting. for control and track the function of lighting towers, it relies on IoT and cloud computing. It represents one of the most disruptive innovations, allowing computing scenarios that are omnipresent. Internet of thing is described by tiny, widely distributed real-world items with fixed storage and processing ability that involve issues of accuracy, efficiency, safety, and particularity [3]. It features a smart development of the playground that supports IoT to evaluate application requirements and recommend architecture for the cloud of things. This is achieved by incorporating the connections with the surrounding world between new-generation services, where the following is centered here: 1- Designing a piece of common evidence to merge the cloud with the IoT. 2- Developing and testing the application based on the IoT and the cloud. 3- Developing devices for this work to facilitate interactions with smart devices using the cloud. 4- Improving in the mechanism of work and making the exchange of data-efficient using JavaScript [6]. The Internet of Things is a term rich with many specifics and modern technologies that, luckily, are set to change life dramatically in our modern world. This means that the IoT is a wide community of devices that are interconnected used to collect and exchange information between devices and to store, evaluate, or analyze the effects of that information [7]. Stadium operators are in a squeeze game between customers expecting a more immersive experience and host stadium seeking higher returns on the dynamic investments of their sport. They need to find new ways to fill the arena, push fans to spend more, and keep everyone healthy with today's advanced home entertainment systems and the latest stats and alerts available on mobile devices [3].

2. CLOUD COMPUTING

Over the past few years, cloud computing has emerged as a transformative model with the potential to convert IT companies and make them more flexible and lither than no prior. Cloud computing can especially allow complex organizations such as stadiums to operate more effectively, create new opportunities, and open new business models because of its numerous and important advantages. The debate about how cloud computing can enable stadiums to become smart has revealed a multitude of applications, in any way of the size and level of organization and resources of a community, albeit obviously at an early stage. [4]. Economic advantages, pace, nimbleness, versatility, high elasticity, and more creativity are promised by Cloud Computing. The organizations reasons for migrating their apps to the Cloud are nearly connected to the next main features of Cloud [4]. There are five important countenances of cloud computing listed below, by depended on the report of the National Institute of Standard Technology. [5]:

- Broad Network Access. Cloud computing services are ready and deliver over the network and are utilized through much client apps for various types of platforms such as PDAs and mobile phones. Resource Pooling. The services of the provider are gathered to be used by various clients using a form of multi-renter with various resource allocated and assigned dynamically according to the order of the client.
- Cloud computing elasticity has an infinite number of services; at any time and quantity, these resources can be delivered from provider to customer. As the application load increases and vice versa, the given resource can be automatically increased.
- Measured Service Although several different clients (such as multi-tenancy) share and pool computing resources, the cloud infrastructure can use appropriate mechanisms to calculate what resources have been used by each individual client. The hiring rate varies from one cloud provider to another.

2.1 Cloud Computing Ingredients

Cloud computing have three basic Ingredients as follows [6]:

- Client Computers: Using client computers, the end-user may communicate with the cloud.
- Distributed servers: they are servers spread between various locations but behave as though they were working together.
- Data Centers: The compilation of servers are the data centers.

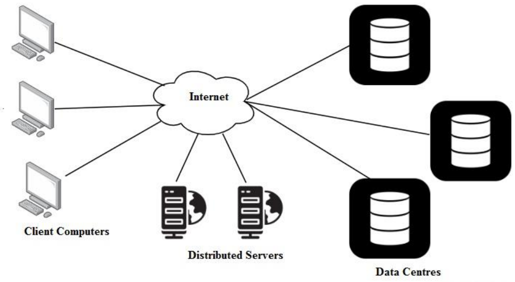


Figure 1. Ingredients of Cloud Computing

2.2 Cloud Computing Services

The cloud infrastructure can be split into the front end back end the and. The front end is made available to the user over Internet connection, allowing the system to communicate with the user. [7]. The back end includes the different models of cloud services:

- Software as a Service. (SaaS)

  The user is given a hosted collection of software working on a platform and infrastructure owned by the cloud provider. Apps are planned and built to be accessed over the Internet by different cloud customers at the same time. CSP, which maintains and ensures the up to date working of the system, manages the hosted program. Multitenancy is provided by the hosted framework, is ready on-request, and can be scaled up to down. Some SaaS providers operate on PaaS or IaaS offerings from other cloud providers. [7]. Example of SaaS: Email and Office output: Email apps, word editors and processors, spreadsheets apps, presentations apps are model examples in this denomination. [8].

- Platform as a Service (PaaS)

  PaaS is a development service that is provided to users through the Internet. No software installation or hardware specifications are required by the user, thereby saving costs. It is a middleware that has built-in tools, built-in protection, and web service interfaces for the deployed applications on which PaaS applications are built. You can integrate the deployed application on the same platform with other applications and interface it with else apps outside of the platform. “PaaS” has software combine a database, middleware, and evolution material.[7]. proverb of “PaaS” [8]:

  a) Application Deployment.

  b) Database.

  c) Development and Testing.

  d) Business Intelligence.

  e) Integration.

- Infrastructure as a Service. (IaaS)

  These is the distribution of servers as a service, storag, network, and operating system. IaaS requires an imaginary computer that the operating system has formerly installed and formation. IaaS enable the storage of data in different geographical location. Providers monitor cloud data center operations while enabling users to implement and manage computing services themselves with flexibility. The user has arrival to virtual machines, storag, network infrastructure, device deployment, and running computing resources. The cloud provider handles only SW and HW, such as servers, host OS, storage devices and virtualization hypervisors. A standard graph of the cloud architecture available to cloud users [7]. Ex. of I-a-a-S [8]:

  a) Content Delivery Networks: To enhance system rendering, such as velocity and cost linked with the acceptance of content for web-based applications, CDNs recording user content and files. This is helpful in handling various types of content for any websites or mobile apps.

  b) Backup and Recovery: This offers the capability to backup and restores files seamlessly.

  c) Compute: This requires server specifications to manage cloud services that can be dynamically purvey and configured.

d) Storage: Storage that is extremely scalable capacity is also available for recording application activities, file backups, and file recovery and storage.

3. INTERNET OF THINGS (IOT)

Smart and self-formation nodes connected in complex and universal network infrastructure are the foundation of the IoT paradigm. It is one of the most innovative inventions for universal and popular computing scenarios.

Internet of Things is the true world and tiny items with restricted storage and processing ability and consecutive issues of fineness, efficiency, protection, and singularity are generally [9]. The IoT is a network that, according to specified agreements, via RFI, infrared sensor, universal position systems, laser scanner, and other datum-sensing devices, it intelligently recognizes, locate, track, monitor, and manages objects. [10]. The awareness layer, the network layer, and the apps layer are included in the basic Internet of things architecture; see Figure 2 [11].

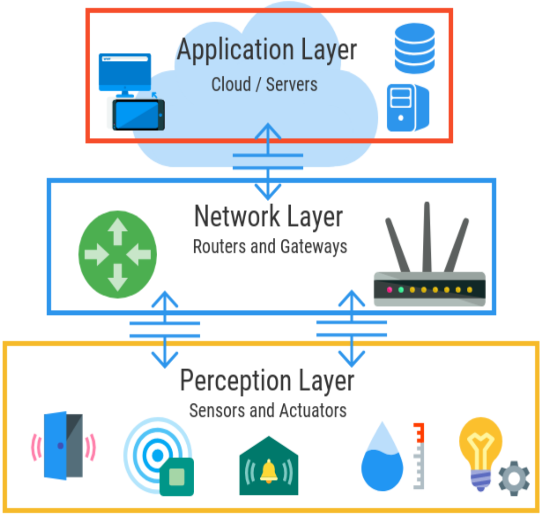


Figure 2. The Basic Architecture of IoT

- Perception layer: To fix the issue of data collecting in the material world and to realize the target of detailed data perception, the perception layer first Collecting data from the outer material environment over cameras, sensors, and other devices. The principal technologies of the perception layer include (RFID), sensor networks, and so on.[11],[12].
- Network layer: Data obtained in the network layer is distributed over current Internet, the connection web, the radio and tv networks, the different arrival networks, and special networks. The transport layer's core technologies are far- reaching wire and wireless connection protocols, network incorporation technology, and intelligent mass information processing technology.[11].
- Application layer: To obtain a wide variety of smart apps solutions, like Smart Stadium and smart transmission, the apps layer combines IoT technology with real industry apps. [13], [11]. see Figure 3. Intelligent computing technologies like edge computing, cloud computing, machine learning, and so on are the main technologies in the application layer.

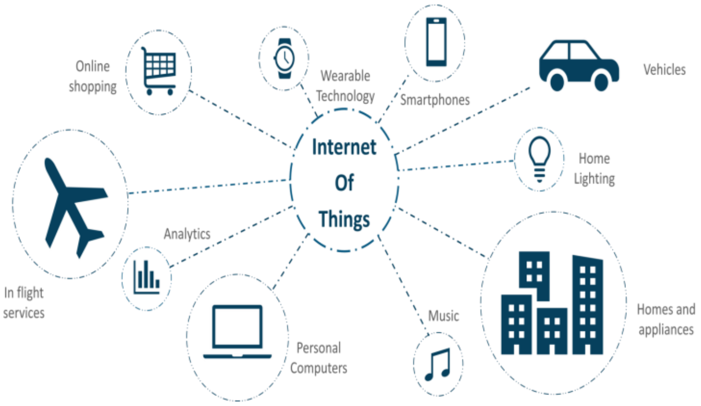


Figure .3 Different Apps of IoT in Human Life

3.1 Technologies of IoT

Different IoT classification technologies are used, but the four prime techniques are as follows: [14]:

a) Radio Frequency Identification “RFID”.

b) Machine to Machine Communication “MtoM”.

c) Vehicle to Vehicle Communication “VtoV”.

d) Near Field Communication “NFC”.

a) Radio Frequency Identification “RFID”.

RFID itis a system consisting of two components: a data-containing wafer and a reading interface. The number of individuals assessed is dependent on the method of granting entry to the building. A simple estimate of space use can be provided by calculating the number of check-ins [15]. RFID technology is based on readers and tags, as we have already mentioned, so RFID describes three configurations in the initial research stage.[14]: -

- active RFID.
- passive RFID
- active Reader Active Tag.

b) Machine to Machine Communication

M2M The referred is to connection among computers, embedded processors, smart sensors, actuators, and mobile devices. In this case, the use of M2M connection is increasing at a quick rate. For example, researchers estimated that, except for mobile phones, yon will be 1.5 billion wireless linked devices by 2014. Currently, there are almost. 2 billion wirelessly linked devices that can collect information from the sensors, analyze that information, and send the information to other devices to implement some mission. The device receives the information and executes task with the assistance of triggers, sensors, embedded processors, and apps software.[14].

c) Vehicle to Vehicle Communication

In that technique, the objects are cars, that can connect with other car or the sensors around there. The key point of worry here is that, since the object move and interacts with else movable object or for the sensors at the wayside, there is no proper method of specifying the protocols. So, we are unable to identify any protocol for routing. This interaction will function for a long distance and create successful contact between objects'. This technology was mainly developed for the purposes of transit control, protection, and prevention of accidents. [14].

d) Near Field Communication (NFC)

NFC is it integrates an RFID reader into a mobile phone, somehow a bit like RFID, which makes it faster, more secure, and more effective for users. NFC is a low-extent wireless technology for a hesitation of 13.56 MHz, work for so short distances up to 4 cm. Complementing Bluetooth and 802.11 with the tall-extent capabilities at a range of above at 10 cm, NFC allows for conjectural initialization of wireless networks. It was first founded by companies such as Philips and Sony. The exchange of data was approx. 424 kbps. In NFC, during data reading, energy exhaustion is beneath 15ma.In NFC technology, there are two modes [14]: Active. Passive.

4. CLOUD AND IOT: THE NEED FOR THEIR INTEGRATION

The cloud world and IoT world have visible a fast and separate development. Both world are so unlike from any other and, until best, they features are also complement, as Table 1 implies. The main explanation of why much researchers have propose and are proposing their integral is such complementarity, usually to gain benefits in specific applications [9].

Table 1. Aspects of Cloud and IoT

	Internet of Things	**Cloud Computing**
Displacement	Pervasive	Centralized
Reachability	Limited	Ubiquitous
Components	Real word "things"	Virtual
Computational capabilities	Limited	Virtually
Role of the Internet	Point of convergence	Means for delivering services
Big data	Source	Means to manage

In general, Internet of things can take feature of the Cloud's nearly infinite capacities and resources to compensate for its technical shortcomings for instance storage, processing, communication. Cloud may provide an efficient sol for IoT operation, department, and installation as well as for execution apps and services that take advantage of the stuff or data generated via them. On the different part, the Cloud would interest of IoT via expansion itis range to deal with real world things in a extra distributed and dynamic way, and to offer new services in a wide variety from real life scenarios.

In Tab.2, the finished Cloud and IoT feature emerging from the various literature proposals and exciting the Cloud IoT paradigm are reported.

Table 2. Complementarity and Integration of Cloud and IoT

IoT	**Cloud**
Pervasive (things placed everywhere) Ubiquitous (resources usable from everywhere)	Ubiquitous (resources usable from everywhere)
Real world things Virtual resources	Virtual resources
Limited computational capabilities Virtually unlimited computational capabilities	Virtually unlimited computational capabilities
Limited storage or no storage capabilities Virtually unlimited storage capabilities	Virtually unlimited storage capabilities
Internet as a point of convergence Internet for service delivery	Internet for service delivery
Big data source Mean to manage big data	Mean to manage big data

- The problems solved and the benefits achieved by implementing the Cloud IoT paradigm are described below [16]:
- Storage resources. IoT offers a broad range of sources of information "like, stuff" with three Big Data features that generate a large amount of nonstructured or semi structured data: volume "like, data size", variety "like, data types", and velocity "like, data generation frequency".
- Computational resources. IoT systems have restricted resources for processing and don't allow data processing on- location. Data composed is typically transmitted to extra efficient nodes where it is possible to aggregate and process, but without proper infrastructure, scalability is difficult to achieve.
- Communication resources. One of the IoT specifications into allow IP_enabled devices to connect via dedicate hardware, and it can be very costly to support such communication. Cloud provides an easy and affordable solution that uses personalized portals and built-in apps to link, monitor, and manage something from anywhere and anytime.
- New capabilities. Very height frequency from devices, technologies, and protocols characterizes the IoT. It can therefore be very hard to obtain scalability, interoperability, reliability, performance, availability, and security.

5. SMART WEB APPLICATION IN SMART STADIUM

One of the findings of the case study was that the knowledge produced by the instruments could be better used to monitor the stadium and around it. And optimize the advantages of the tools through this. An application that can be used by Stadium management often offers useful feedback, as seen by the Edge Olympic, for the data lake. These could have a beneficial effect on the declared objectives for each smart device, however on cost reduction and user experience support. This type of approach can easily be implemented on the network if a stadium has a rigid basic infrastructure. [15].

IoTCloud is an open-source project aim at merge stuff (smartphones, tablets, robots, websites, etc..) with background to handle sensors and they messages and to provide an API for apps that are concerned in these data. The Cloud may provide an efficient solution for implementing the management and composition of IoT resources as well as applications that take advantage of stuff or data generated by them.[9]. CloudIoT has given origin to a new collection of intelligent services and apps so as to can have a huge effect on daily life as shown in. Figure .4[9].

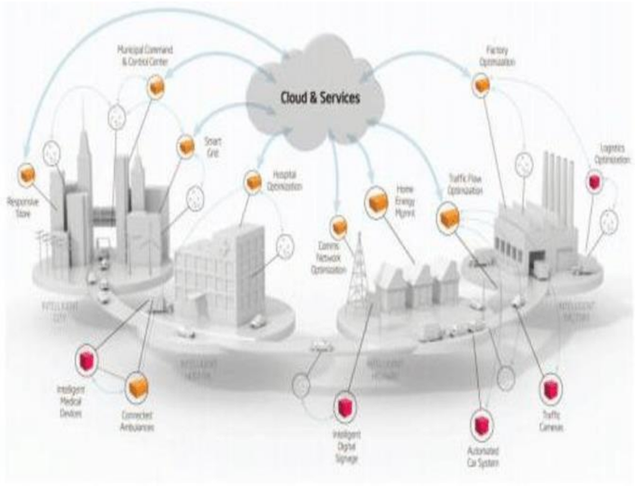


Figure 4. Services made potential thanks to the CloudIoT paradigm

Three layers are used in the standard web application: presentation, application, and database. However, you usually see the presentation layer divided into two separate layers when dealing with stable and modular web applications: client and representation. Figure.5 shows the three_tier web pattern [17].

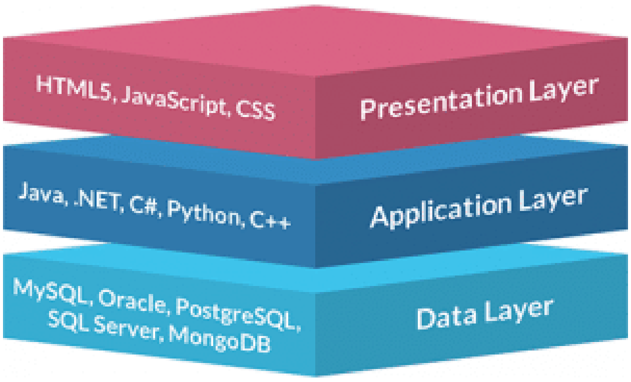

HTML5, JavaScript, CSS
Presentation Layer
Java, .NET, C#, Python, C++
Application Layer
MySQL, Oracle, PostgreSQL, SQL Server, MongoDB
Data Layer

Figure 5. The Three tier_web_pattern

a) The- tier - web pattern

It is crafted to relief developers to read the core components of the framework for developers to make it more flexible and scalable. This architecture is planned to have an overall public-facing interface. By divide an app into many levels, he can install middleware, safeguard every individual layer, and until give up layers to untrustworthy third-party apps. [17]. Figure.6 show an alternate version of the tiered web style that splits the presentation layer to two layers. The developer will offload the client layer to the individual client by breaking the display layer into the client and representative layer to effectively provide several different clients with a single representation.

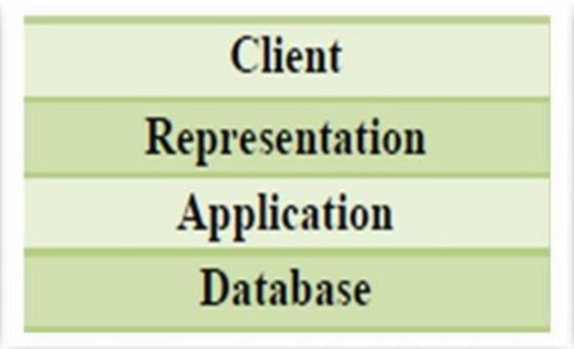


Figure 6. The four tier web pattern

b) Reasons for Usage

If any of the above applies, the developer wants to use this pattern: Needed to build a modular cloud system. To have many interfaces for his system. And link different apps to every other (using Amazon cloud services, Google Cloud... etc.). [16].

c) Implementation

A standard implementation of an n tier architecture is based on a four-tier architecture. The most significant thing is whither each layer goes...Figure.7 illustrates how much a develop can divide the layers that it cloud services offer.

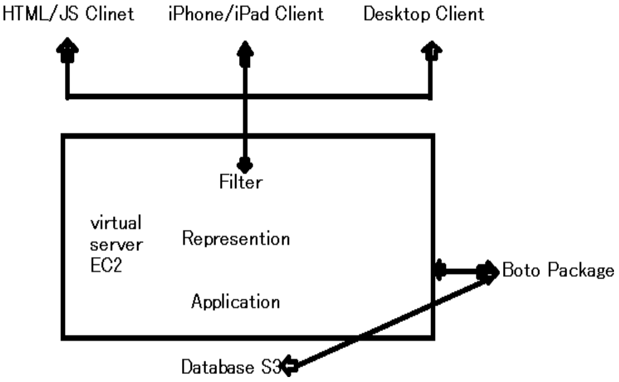


Figure7. Deployment of the n-tier architecture

In the 'n'-tier architecture system, three distinct client layers are given: one for basal HTML and JScript, the other for iPhone clients device and iPad clients device, and a tertiary for desktop clients. Each of this three layers will sitting the user with the data and set it up directly on the client's device. A developer has almost no faith in anything coming from either of these clients, so all authentication and authorization below this layer must be done by a programmer. The candidate layer that allows a developer to recap the authenticate and license from the representation and app layers is straight underneath client layers. It sits direct on top of the layer of representation, altering any input and output flowing in which. Both two layers need to talk same protocol of communication.

6. LITERATURE SURVEY

Looking to the smart stadium's institutional context helps us positioning the overarching rationale of innovation crisscrossing the "permeable boundaries" of the stadium, who no way to stands alone in the analysis. We discuss how the stadium is built by the IoT and Cloud Computing techniques and university projects, which serve as an information infrastructure that conditions those facts, techniques, and smartness narratives to be applicable in the present.

S. Panchanathan et al [1] The Authors discuss here on three fan enrichment initiatives were presented within the framework of the Smart Stadium for Smarter Living action. These ventures centered on enhanced protection Crowd Under-standing, fan participation Sporty Demonstrator Platform, and deficiency /convenience (Wait Time/Queue Estimation). Each data collection was split into a classified training set and an unclassified set randomly. 10 percent of the dataset size was set to the batch size. From the unclassified set, a batch of samples was queried, appended to the classified collection, and the output was assessed on entire unclassified collection.

M. M. Froufe et al.[2] The Authors discuss here on proposes that the key drivers and systems of smart buildings be identified and compared by associating them with the main beneficiaries: consumers, owners, and the climate. On the basis of the approach adopted, 11 drivers and eight systems have been identified and drivers have been grouped into three groups from the study of the key beneficiaries: consumers primarily concerned with health, wellbeing and meeting expectations; owners primarily concerned with improving the cost benefit ratio; and the environment primarily concerned with reducing consumption and pollution. The analysis had three main objectives: first, to discuss the main drivers that improve the knowledge of a building by rating them according to the main beneficiaries; second, to investigate the main systems that are sitting in those buildings; and third, to investigate the relationship between drivers and systems. We used a three step way to achieve these objectives:

bibliographic scan, identification of the smart building's key drivers and systems, and find of the relationships between drivers and systems.

S. A. Alhadad et al [3]. The Authors focus here on Addresses the importance of the use of specialized equipment in the area of a sports organization. It starts with an introduction of how, with live examples, they are of a paramount benefit to either the fans of the stadium's infrastructure facilities, e.g., Parking lot entrance, the ability of the controlling smart systems to detect any emergency or defect to handle the problem at once. After that, how the information security system work in the stadium, accompanied by exclusive and unique pictures and graphics. Three producers are essential in the first stage, cameras, sensors, and the IoT gateway. Cloud analytics rabidly capture and evaluate them, allowing stadium managers to make data-driven decisions.

C. Kakderi et al [4]. The authors also concentrate on the STORM CLOUDS model as a sol for municipalities everywhere (1) deploying a purse of governance, economic and quality of life smart city applications on a single cloud-based platform, and (2) using the platform and its corresponding resources to move their current appls to the cloud environment. It plays an important role in making efficient use of services that are distributed. Also discussed was the expansion of SCP for the rapid deployment of sensors and motors connected to the network at the city level and three modern modules must be developed to back up the basic reform of IoT solutions. 1- The control unit will deal with the interface of the device and enable the risky response in time as it is composed of the interface and the operating system. 2- A data provisioning unit that provides a unified acquisition of sensor data to enable additional processing steps as it will store the data obtained from the SCP data service layer. 3- The Big Data Analytics Unit will provide real analytics, identify data of interest, and improve algorithms and services.

M. U. Bokhari et al [5] The authors focus primarily on the concept of cloud computing technology and different levels of cloud architecture. Also, cloud service and implementation models are discussed briefly. Comparison of different cloud computing services models, implementation models: private, public, and community cloud, as well as public and private cloud information security specifications according to different service models, have been provided. Cloud computing, however, has many features, including on-demand self-service, large network connectivity, pooling of resources, elasticity, and calculated service, but it cannot be fully trusted. Finally, the main challenges and issues of cloud computing with regards to security for further research have been discussed in the chapter.

P. Srivastava et al [6]. The authors focus primarily on the brief review of the implementation, development, forms, and components of cloud computing in cloud computing, as well as various cloud computing methods and some of its benefits. The cloud computing application area will be gradually rising. Cloud computing is now used by almost all small and large industries to handle storage, traffic, and hardware requirements.

Odun-Ayo et al. [7]. The key objective of the authors is to define, analyze and clarify the emerging developments and growth in the architecture of cloud computing.

A. Botta, W. De Donato, V. Persico, and A. Pescapé.[9] The Authors focused on how we integrate cloud computing and the Internet of Things, or what we call CloudIoT. And look for important challenges such as hardware and technology inconsistencies, hardware, reliability, scalability, and safety. He also showed that the CloudIoT model is related to energy, energy efficiency, etc.

J. H. Nord et al [10] The authors focused on establishing an extensive review and explanation of the IoT, including discussion of IoT architecture, applications, and impact. In addition, IoT priority areas challenges were identified, and a theoretical framework and conceptual model-based.

G. Mei et al. [11] The authors concentrated on IoT implementations, innovations, and problems in the protection of geo-hazards. The IoT is commonly use in the preventing of three collective classifications of geo-hazards: (1) collapse of slopes, include landslides, flow of debris and Rocks (2) surface deformation, include surface clefts, collapsing of surfaces and decline of surfaces, and (3) Earthquakes. Risks. The emphasis was on providing a detailed survey of applicable IoT research and technical advances related to the prevention of geo-hazards. In the monitoring and early warning of seven types of common geo-hazards, including landslides, debris flow, rockfall, soil subsidence, surface collapse, surface cracks, and earthquakes, it first surveys the IoT implementations, then examines the main geo-hazard mitigation technologies while using the IoT. And the concerns of IoT-based tracking and early warning systems for geo-hazard avoidance are finally summarized. Furthermore, the possible recommendations for using the IoT for the protection of geo-hazards are also illustrated.

A. Tiwary et al [13] The authors concentrated on IoT and its applications in various science and technology fields. It is also given alongside the launch of the IoT literature review. It also addresses the design and components of the IoT along with its various applications. Architecture and various IoT elements are clarified. It also defines the main features and their implementations.

S. van Heck [15] focused on the following research question to be answered in this study: what smart instruments maybe found in stadiums, and how much can this smart tools be configured for use? And address the stadium-focused questions: what smart tools maybe found in stadiums, and how can to be configured to use these smart tools? To maximize the use of the tools, what interventions can be recommended? What progress has been made since the advent of intelligent tools, and what can be improved? What smart tools are implemented at a stadium and what are the targets to their integration? What features do smart stadiums have? What are the features of a stadium and how does the need for smart tools apply to this? How is the integral of smart tools concerning to real ownership management theories? What are smart tools?

M. Puneet et al [17] The authors concentrated on how to develop any cloud web application, provide multiple interfaces for it, and how to select the best Amazon Web Services service for an application. The authors concentrated on how to develop any cloud web application, provide multiple interfaces for it, and how to select the best Amazon Web Services service for an application. And if developers want to use Amazon cloud services and can easily create applications using the cloud, the cost of cloud computing is also small since all the software and hardware available are leased from cloud services for use time and high performance that the application obtained from cloud services.

7. CONCLUSIONS

The growth of IoT software is turning our environment into one previously considered impossible. The IoT will service our community by growing efficiency, integrity, and convenience for both businesses and consumers alike. However, Internet of things involves key legal concerns for any new technology, such as protection, privacy, data management, and the need for standards and protocols. If left unchecked, the IoT could have passive effects. If dealt with successfully, however, the IoT will flourish while maintaining individuals' fundamental rights. newly, sensors with high sensibility and low price are on the market. With the evolution of the Internet, we can send and receive data anywhere in the world. In addition, device and storage virtualization and software-defined network development enable the efficient use of ICT for infrastructure in many fields. Technologies and principles in various areas, such as civil engineering and ICT, will be integrated in the near future. In addition, social infrastructures would be virtualized by ICT in the real world. A smart society can then be realized where, by accurate data analysis and control, we can run the infrastructure. The cost of cloud computing is also small since all the software and hardware required is leasehold-for-use time as well as high execution performance that the app acquires from cloud providers, and we can easily develop the application using the cloud.

8. REFERENCES

[1] S. Panchanathan et al., “Enriching the fan experience in a smart stadium using internet of things technologies,” Int. J. Semant. Comput., vol. 11, no. 2, pp. 1–34, 2017, doi: 10.1142/S1793351X17002751.

[2] M. M. Froufe, C. K. Chinelli, A. L. A. Guedes, A. N. Haddad, A. W. A. Hammad, and C. A. P. Soares, Smart Buildings: Systems and Drivers, vol. 10, no. 9. 2020.

[3] S. A. Alhadad and O. G. Abood, “Enhancing Smart Sport Management based on Information Technology,” IOSR J. Sport. Phys. Educ. (IOSR-JSPE, vol. 5, no. 5, pp. 19–26, 2018, DOI: 10.9790/6737-05051926.

[4] C. Kakderi, N. Komninos, and P. Tsarchopoulos, “Smart cities and cloud computing: lessons from the STORM CLOUDS experiment,” J. Smart Cities, vol. 2, no. 1, 2016, DOI: 10.18063/JSC.2016.01.002.

[5] M. U. Bokhari and Q. Makki, “A Survey on Cloud Computing A Cloud architecture A Security,” pp. 149–164, 2018.

[6] P. Srivastava and R. Khan, “A Review Paper on Cloud Computing,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 8, no. 6, p. 17, 2018, DOI: 10.23956/ijarcsse.v8i6.711.

[7] I. Odun-Ayo, M. Ananya, F. Agono, and R. Goddy-Worlu, “Cloud Computing Architecture: A Critical Analysis,” Proc. 2018 18th Int. Conf. Comput. Sci. Its Appl. ICCSA 2018, pp. 1–7, 2018, DOI: 10.1109/ICCSA.2018.8439638.

[8] H. opencrowd. co. Cloud Taxonomy .

[9] A. Botta, W. De Donato, V. Persico, and A. Pescapé, “Integration of Cloud computing and Internet of Things: A survey,” Futur. Gener. Comput. Syst., vol. 56, pp. 684–700, 2016, DOI: 10.1016/j.future.2015.09.021.

[10] J. H. Nord, A. Koohang, and J. Paliszkiewicz, “The Internet of Things: Review and theoretical framework,” Expert Syst. Appl., vol. 133, pp. 97–108, 2019, DOI: 10.1016/j.eswa.2019.05.014.

[11] G. Mei, N. Xu, J. Qin, B. Wang, and P. Qi, “A Survey of Internet of Things (IoT) for Geohazard Prevention: Applications, Technologies, and Challenges,” IEEE Internet Things J., vol. 7, no. 5, pp. 4371–4386, 2020, DOI: 10.1109/JIOT.2019.2952593.

[12] P. P. Ray, “A survey on Internet of Things architectures,” J. King Saud Univ. - Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, 2018, DOI: 10.1016/j.jksuci.2016.10.003.

[13] A. Tiwary, M. Mahato, A. Cheddar, M. K. Chandrol, M. Shrivastava, and M. Tripathi, "Internet of Things (IoT): Research, Architectures, and Applications," Int. J. Futur. Revolut. Comput. Sci. Commun. Eng., vol. ISSN, no. 4, pp. 2454–4248, 2018, [Online]. Available: http://www.ijfrcsce.org.

[14] V. K. B., S. L. Joshi, and S. H. Barshikar, “A Survey on Internet of Things,” Int. J. Comput. Sci. Eng., vol. 6, no. 12, pp. 492–496, 2018, DOI: 10.26438/ijcse/v6i12.492496.

[15] S. van Heck, "Smart Stadium Tools," no. June 2019, [Online].

Available:https://repository.tudelft.nl/islandora/object/uuid:4e3536e0-f6c3-458c-8ac0-ba81b85a5ba3/datastream/OBJ/download.

[16] J. Angelin Jebamalar and A. Sasi Kumar, “A review on the integration of cloud computing and internet of things,” Int. J. Eng. Technol., vol. 7, no. 2.33 Special Issue 33, pp. 683–684, 2018, doi: 10.14419/ijet.v7i2.33.15475.

[17] M. Puneet, J. Kaur, and M. Pallavi, “International Journal of Software and Web Sciences (IJSWS),” no. October 2016, pp. 54–57, 2013

IoT an Overview: Advantage, Disadvantage and Applications

Bhagwati Charan Patel
Department of Information Technology, SSTC, SSGI
Bhilai, India

Ram Shankar Tripathi
Scholar
Department of Information Technology SSTC, SSGI
Bhilai, India

Naveen Goel
Department of Electrical and Electronics Engineering,
SSTC, SSGI
Bhilai, India

Abstract: Internet of Things (IoT) is a well-known term that has gained massive encouragement over a few years. The future of the human race will be significantly influenced by the application of IoT over the coming years. The Internet is everywhere and touched almost every corner of the globe affecting our lives in previously unimagined ways. As a living entity, the Internet is constantly evolving, and now, an era of widespread connectivity through various smart devices (i.e., things) that connect with the Internet has begun. IoT looks more like an umbrella covering many protocols, technologies, and concepts that depend on specific industries. It will lead to the development of efficient mechanisms with high scalability and interoperability features among the things or objects. IoT is a reality that is progressing day by day, connecting billions of people and things to form a vast global network. IoT has applications in various domains like agriculture, industry, military, and personal spaces. There are potential research challenges and issues in IoT that act as a hurdle in the complete exploration of IoT in real-time implementation.

Key Words: Internet of Things, IoT architecture, RFID, Smart technology, Cloud computing, WSN

1. INTRODUCTION

The Internet of Things (IoT) is a kind of network which is created by the different devices performing separate tasks for some common purposes. We are entering an era of the “Internet of Things”. This term has been defined by different authors in many different ways. Let us look at two of the most popular definitions. Vermesan et al. [1] define the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators. Another definition by Pe˜na-L´opez et al. [2] defines the Internet of Things as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object. Main components [3] of IoT are sensors and physical objects. With the help of Wireless sensor Network and RFID, information is exchanged in this era of internet of things every device is uniquely identified. Sensors and actuators are devices, which help in interacting with the physical environment. The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it. Note that we broadly define the term sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment). An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner and accessed to the network [4].

IoT is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established. Over 9 billion ‘Things’ (physical objects) are currently connected to the Internet, as of now. In the near future, this number is expected to rise to a whopping 20 billion.

There are four main components used in IoT as shown in Fig. 1:

1. **Low-power embedded systems –** Less battery consumption, high performance are the inverse factors play a significant role during the design of electronic systems.
2. **Cloud computing –** Data collected through IoT devices is massive and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
3. **Availability of big data –** We know that IoT relies heavily on sensors, especially real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
4. **Networking connection –** In order to communicate, internet connectivity is a must where each physical

object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

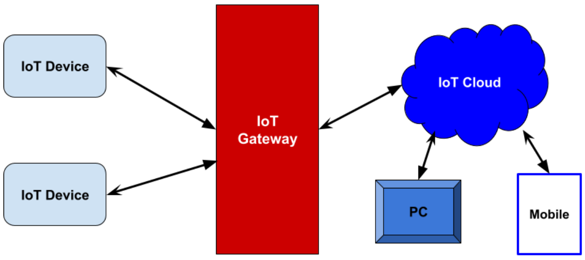


Fig. 1 IoT Structure

2. ARCHITECTURE OF IOT

The layered architecture in context of IoT has five layers named business, application, middle, network, and perception layers [5-8] as shown in Fig. 2.

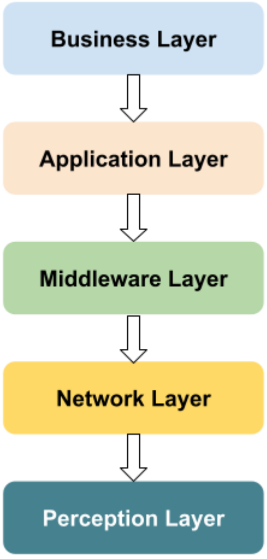


Fig. 2 IoT Architecture

1. Business Layer: Once IoT data is procured, it is valuable only if it applies to business planning and strategy. Every business has specific goals and objectives that it wants to accomplish by gathering intelligence from data. Business owners and stakeholders use data from past and present data to plan precisely for the future.

2. Application Layer: In this layer, Data is further processed and analyzed to gather business intelligence. Here IoT systems get connected with middleware or software that can understand data more precisely.

3. Middleware Layer: It transports data from sensor to control rooms for processing the information safely. It serves the requests taken from the network layer. There is data base which may be used if needed to perform ubiquitous computing and decision making about the results. The SOA architecture of IoT has applications, service management, service composition, object abstraction objects [9-12]. Apart from this it needs a trust, privacy, and security management.

4. Network Layer: The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.

5. Perception Layer The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

3. IOT − KEY FEATURES

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below:

Artificial Intelligence – IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favourite cereal run low, and to then place an order with your preferred grocer.

Connectivity – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

Sensors – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

Active Engagement – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

Small Devices – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

4. CHALLENGES

This emerging IoT has tremendous usages as well as dangers also, as it connects with the physical world. Internet threat today steals credit cards. Who can tell that future internet will not ruin home security system and disrupt hospital? Different heterogeneous devices connecting to each other in unsupervised way giving birth of insecurity of internet operation. Two important issue/challenges of IoT can be low power and security function. There are lot of vulnerabilities in IoT because of its nature of network [13-15]. The security requires resilience to the attacks, access control, data authentication, and client privacy.

5. ADVANTAGES OF IOT

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer:

- Improved Customer Engagement – Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.
- Technology Optimization – The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.
- Reduced Waste – IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
- Enhanced Data Collection – Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

6. DISADVANTAGES OF IOT

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Here is a list of some its major issues:

- Security – IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
- Privacy – The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
- Complexity – Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.
- Flexibility – Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
- Compliance – IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

7. PRACTICAL APPLICATIONS

The versatility of IoT has become very popular in recent years. There are many advantages to having a device based on IoT. Mckinsey Global Institute reports that IoT business will reach 6.2 trillion in revenue by 2025. There are lots of applications are available in the market in different areas.

(i) Personal Home Automation System: Home Automation system is the major example in this area.

Wemo Switch Smart Plug: It is the most useful devices which connected home devices in the Switch, a smart plug. It plugs into a regular outlet, accepts the power cable from any device, and can be used to turn it on and off on hit a button on your smartphone.

(ii) Enterprise: In the enterprise area many applications are there like environmental monitoring system, smart environment etc.

Nest Smart Thermostat: It is connected to the internet. The Nest learns automatically your family’s routines and will automatically adjust the temperature based on your activities, to make your house more efficient. There is also a mobile app which allows the user to edit temperature and schedules.

(iii)Utilities: smart metering, smart grid, and water monitoring system are the most useful applications in the various utility area.

(iv)Energy Management: Advanced Metering Infrastructure is the major example in this area.

(v) Medical and Health Care: Remote health monitoring and emergency notification system are examples of IOT in the medical field.

Health patch Health Monitor: It can be used for the patient who can’t go to doctors, letting them get ECG, heart rate, respiratory rate, skin temperature, body posture, fall detection, and activity readings remotely.

(vi) Transportation: Electronic toll collection system is the most useful example in this area.

(vii) Large scale deployment: There are various large projects ongoing in the world. Songdo (South Korea), the first of its kind fully wired Smart City, is near completion. Everything in this city is planned to be wired, connected and turned into a data stream that would be monitored by an array of computers without any human interaction.

8. CONCLUSIONS

This paper surveys the IoT standards, technology, architectures, and enabling technologies of the IoT with special attention of security, privacy, and trust aspects. Various techniques and ways are described and analysed on the basis of important parameters. Treats, attacks and vulnerabilities of various levels are analysed.

REFERENCES

[1] O. Vermesan, P. Friess, P. Guillemin et al., “Internet of things strategic research roadmap,” in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.
[2] I. Pe˜na-L´opez, Itu Internet Report 2005: The Internet of Things, 2005.
[3] Louis COETZEE1, Johan EKSTEEN2,"The Internet of Things –Promise for the Future? An Introduction", IST Africa 2011 Conference Proceedings
[4] O. Said and M. Masud, “Towards internet of things: survey and future vision,” International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.
[5] Khan R, Khan SU, Zaheer R, Khan S. Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on 2012 Dec 17 (pp. 257-260). IEEE.
[6]. Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on 2012 Mar 23 (Vol. 3, pp. 648-651). IEEE.
[7]. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018 May 1; 82: 395-411.
[8]. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 2014 Nov 1; 20(8):2481-501.
[9]. Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28;54(15):2787-805.
[10] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of internet of things,” in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE ’10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.
[11] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future internet: the internet of things architecture, possible applications and key challenges,” in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT ’12), pp. 257–260, December 2012.
[12] H. Ning and Z. Wang, “Future internet of things architecture: like mankind neural system or social organization framework?” IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.
[13]. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer Networks. 2013 Jul 5; 57(10):2266-79.
[14]. Vasilomanolakis E, Daubert J, Luthra M, Gazis V, Wiesmaier A, Kikiras P. On the security and privacy of internet of things architectures and systems. In Secure Internet of Things , 2015 International Workshop on 2015 Sep 21 (pp. 49-57). IEEE.
[15]. Weber RH. Internet of Things–New security and privacy challenges. Computer law & security review. 2010 Jan 1; 26(1):23-30.

International Journal of Computer Applications Technology and Research
Volume 10–Issue 05, 123-131, 2021, ISSN:-2319–8656

ECC Based Defense Scheme for Selective Drop Attack in Wireless Ad Hoc Network

Sangeetha V
PG Scholar- M.E Wireless communication
PSG College of Technology
Coimbatore, India

Dr. G. Umamaheswari
Associate Professor
PSG College of Technology
Coimbatore, India

Abstract: Performance and security are two critical functions of wireless ad-hoc networks (WANETs). Network security ensures the integrity, availability, and performance of WANETs. It helps to prevent critical service interruptions and increases economic productivity by keeping networks functioning properly. Since there is no centralized network management in WANETs, these networks are susceptible to packet drop attacks. In selective drop attack, the neighbouring nodes are not loyal in forwarding the messages to the next node. It is critical to identify the illegitimate node, which overloads the host node and isolating them from the network is also a complicated task. Resistive to selective drop attack (RSDA) scheme is proposed to provide effective security against selective drop attack. A lightweight RSDA protocol is proposed for detecting malicious nodes in the network under a particular drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANETs such as AODV and DSR. It accomplishes reliability in routing by disabling the link with the highest weight and authenticate the nodes using the elliptic curve digital signature algorithm. In the proposed methodology, the packet drop rate, throughput and end to end delay are analysed.

Keywords: wireless ad-hoc networks; resistive to selective drop attack; network security; elliptic curve digital signature algorithm; distance vector routing; ad-hoc on demand distance vector routing

1. INTRODUCTION

Wireless Ad-Hoc Networks (WANETs) decentralized nature makes suitable for different types of applications, where central nodes cannot be trusted on and may progress the scalability of networks linked to wireless networks, through practical and theoretical confines to the overall size of such networks have been recognized. Minimal configuration and quick deployment make ad hoc networks suitable for emergencies in military or natural disasters conflicts. The existence of adaptive and dynamic routing protocol enables ad hoc networks to be formed quickly [1]. The applications can further classify wireless Ad-hoc networks into Vehicular Ad hoc Networks (VANETs), Mobile Ad hoc Networks (MANETs), Smartphone Ad-hoc Networks (SPANs), Wireless mesh networks. Wireless Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of novel attacks. A black hole attack (BLA) is one of the most typical attacks and works as follows. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs. Wireless networks have many different architectures than that of a typical wired network; a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host can drop packets at will [2]. The RSDA protocol can provide resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination. To address the selective drop attack, a reliable factor is chosen by computing the list of link weights. If the sum of the weight of a particular route is high, e.g., it indicates that the low reliability, the attacking node can be identified. Each node maintains its own weight; the obtained weight is added to the route request payload. By computing the reliability rate, malicious nodes can be distinguished from other normal nodes. The performance of RSDA protocol is increased compared to existing approaches by considering the factors such as packet drop rate, jitter and routing overhead

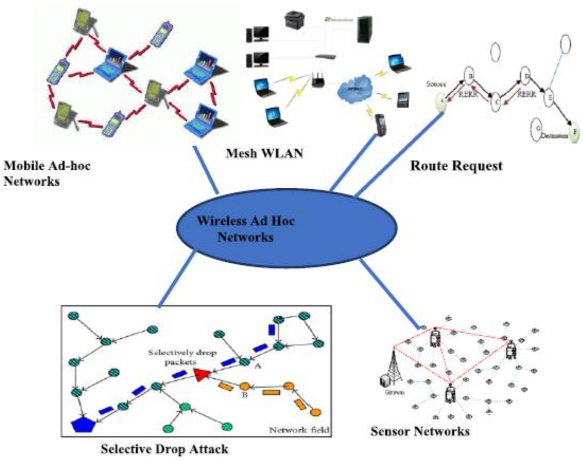


Figure 1. Wireless Ad-Hoc networks (WANETs)

Routing table size is minimized by only including next hop information, not the entire route to a destination node. Sequence numbers for both destination and source are used. Managing the sequence number is the key to efficient routing and route maintenance. Sequence numbers are used to indicate the relative freshness of routing information. Updated by an originating node, e.g., at initiation of route discovery or a route reply. In figure 1 the wireless ad hoc network (WANETS) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring a central device, such as a router or access point. When Wi-Fi networks are in ad-hoc mode, each device in the network forwards data to the others [3]. The RSDA protocol has been designed to offer resistance to selective drop attacks by preventing the nodes from getting overloaded. It achieves reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination. This mainly contributes on Wireless Ad Hoc Networks and their security related issues. A review on various protocols is done to deal with selective drop attack in WANET.A light weight RSDA protocol has been proposed for detecting malicious nodes in the network under selective drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANET such as AODV and DSR. An efficient cryptographic technique ECDSA has been chosen for providing authentication which has a lesser key size however it provides similar security. Finally, it achieves extreme network security measures ensures the integrity, availability, and performance enhanced using RSDA for WANET. In selective drop attack, the malicious nodes would refuse of forwarding message passing through them. At last this attack can potentially drop the throughput of a host to a minimum level. The RSDA protocol has been proposed to strengthen the resistance to selective drop attacks by thwarting the nodes from getting overloaded [4]. It attains reliability in routing by disabling the link as defective or attempts to obtain a new efficient route to the destination.

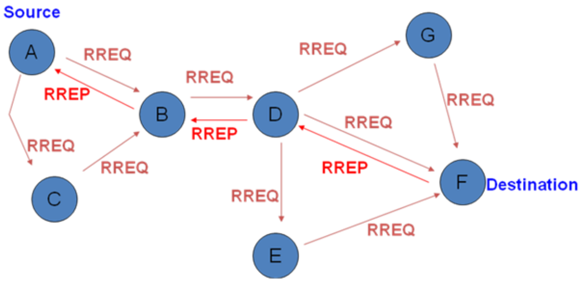


Figure 2. Message routing in AODV

In Figure 2 Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address for the message.

2. PROBLEM STATEMENT

The packet drop attack can frequently be used to attack WANETs. Wireless networks have many different architectures than that of a typical wired network; a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host can drop packets at will. Also over a mobile ad-hoc network, hosts are especially vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other host on the network. This kind of attacks can be detected at an early stage by monitoring few hundreds of packets based on the number of requests that a host receives from a particular host from a fixed interval of time changes. The early detection of DoS attack prevents the controller going down. If detection happens at early stage then, the impact of flooding of malicious packets can be controlled significantly. The early detection mechanism must be of light weight and should have a high response time [5]. The high response time saves the controller in the period of attack to regain the control by terminating the DoS attack.

2.1 Software tools used

Even though there are various tools available to implement the networking technology, the open source software is preferred for its flexible approach towards creating custom algorithms. One such software available to implement the Wireless sensor network test bed is NS2. Network simulation is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/routers, data links, packets, etc.) using mathematical formulas, or actually capturing and playing back observations from a production network. When a simulation program is used in conjunction with live applications and services in order to observe end-to-end performance to the user desktop, this technique is also referred to as network emulation. Most network simulators use discrete event simulation, in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future events such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.

3. IMPLMENTATION

Soft security mechanism was proposed as a fully distributed trust-based public key management technique for MANET. A Composite Trust-based Public Key Management (CTPKM) was proposed to maximize the performance by mitigating the vulnerabilities. A trusted threshold was fixed with each node to decide whether to trust another node or not. A mechanism based on the simple rate-based control packet forwarding mechanism to alleviate malicious control packet was proposed. It was made secure against other DDoS attacks, and those legitimate nodes are not erroneously treated as misbehavior node. Anti Black Hole (ABM) mechanism, which estimates the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node [6]. Multipath forwarding technique to identify attacks in a wireless sensor network based on selective forwarding attack procedure was proposed. Thus it is necessary to propose a strong security based system for IoT based wireless sensor network. Our proposed work handles this effectively. To address the selective drop attack, a reliable factor is chosen by computing the list of link weights. If the sum of the weight of a particular route is high, e.g., it indicates that the low reliability, the attacking node can be identified. Each node maintains its own weight; the obtained weight is added to the route request payload. By computing the reliability rate, malicious nodes can be distinguished from other normal nodes. Unicast delivers a message to a single specified node; Broadcast delivers a message to all nodes in the network; Multicast delivers a message to a group of nodes that have expressed interest in receiving the message; Anycast delivers a message to any one out of a group of nodes, typically the one nearest to the source. RSDA provides an effective security for selective drop attack. It attains reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination [7].

In the below figure 3 represents architecture of proposed system, in which all modules of the work are represented. Wireless network initialized and nodes are assigned with AES and ECC key and verified on message transfer. The design is a plan or drawing produced to show the look and function or workings of an object before it is made. Unified Modeling language (UML) is a standardized modeling language enabling developers to specify, visualize, construct and document artifacts of a software system. Thus, UML makes these artifacts scalable, secure and robust in execution. UML is an important aspect involved in object-oriented software development. It uses graphic notation to create visual models of software systems.

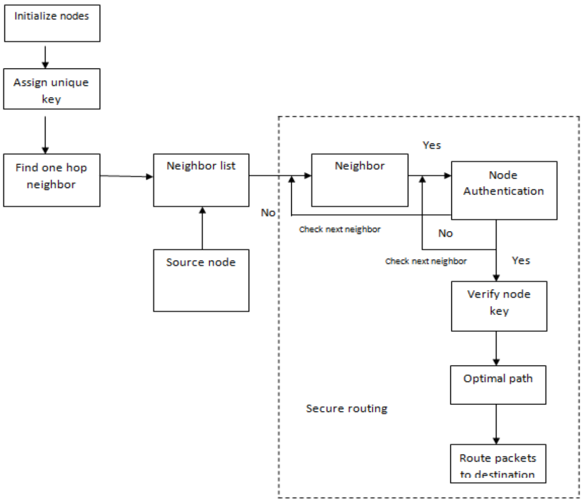
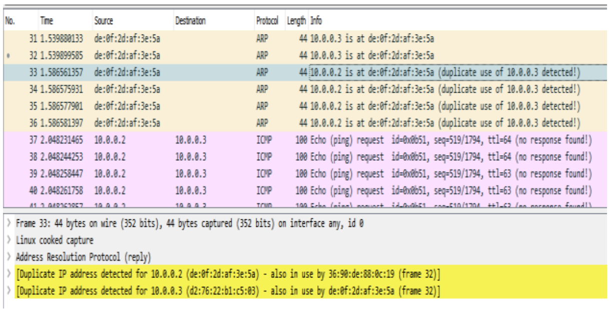


Figure 3. Architecture diagram

Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more. Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify the type of traffic is crossing the network. In Figure 4 it shows the analyzing of duplicate packets using Wireshark.



```
No.   Time          Source              Destination  Protocol Length Info
   31 1.539880133   de:0f:2d:af:3e:5a                ARP       44 10.0.0.3 is at de:0f:2d:af:3e:5a
   32 1.539899585   de:0f:2d:af:3e:5a                ARP       44 10.0.0.3 is at de:0f:2d:af:3e:5a
   33 1.586561357   de:0f:2d:af:3e:5a                ARP       44 10.0.0.2 is at de:0f:2d:af:3e:5a (duplicate use of 10.0.0.3 detected!)
   34 1.586575931   de:0f:2d:af:3e:5a                ARP       44 10.0.0.2 is at de:0f:2d:af:3e:5a (duplicate use of 10.0.0.3 detected!)
   35 1.586577901   de:0f:2d:af:3e:5a                ARP       44 10.0.0.2 is at de:0f:2d:af:3e:5a (duplicate use of 10.0.0.3 detected!)
   36 1.586581397   de:0f:2d:af:3e:5a                ARP       44 10.0.0.2 is at de:0f:2d:af:3e:5a (duplicate use of 10.0.0.3 detected!)
   37 2.048231465   10.0.0.2            10.0.0.3     ICMP     100 Echo (ping) request  id=0x0b51, seq=519/1794, ttl=64 (no response found!)
   38 2.048244253   10.0.0.2            10.0.0.3     ICMP     100 Echo (ping) request  id=0x0b51, seq=519/1794, ttl=64 (no response found!)
   39 2.048258447   10.0.0.2            10.0.0.3     ICMP     100 Echo (ping) request  id=0x0b51, seq=519/1794, ttl=63 (no response found!)
   40 2.048261758   10.0.0.2            10.0.0.3     ICMP     100 Echo (ping) request  id=0x0b51, seq=519/1794, ttl=63 (no response found!)

> Frame 33: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
> Linux cooked capture
> Address Resolution Protocol (reply)
> [Duplicate IP address detected for 10.0.0.2 (de:0f:2d:af:3e:5a) - also in use by 36:90:de:88:0c:19 (frame 32)]
> [Duplicate IP address detected for 10.0.0.3 (d2:76:22:b1:c5:03) - also in use by de:0f:2d:af:3e:5a (frame 32)]
```

Figure 4. Analyzing duplicate packets using Wireshark

Since attacker replicates his own MAC address between target and client, the ARP table gets updated with replicated MAC address. Each switch has an ARP (Address Resolution Protocol) table in order to store the IP addresses and MAC addresses of the network devices. The ARP table is used to determine the destination MAC addresses of the network nodes. Thus by analyzing packets after ARP spoofing, the MAC address gets replicated between the hosts with the different IP address in ARP table. Here, the detection is based on IP-MAC addresses bindings. Once the topology gets initialized, the controller will dynamically allocates MAC address for every IP address in the network. The controller will store that created MAC address in MAC_to_port table. During attack, the attacker duplicates his own MAC address and spoofs arrived packets. But the controller doesn't knows whether arrived packets having legimate MAC address or duplicated MAC address [8].

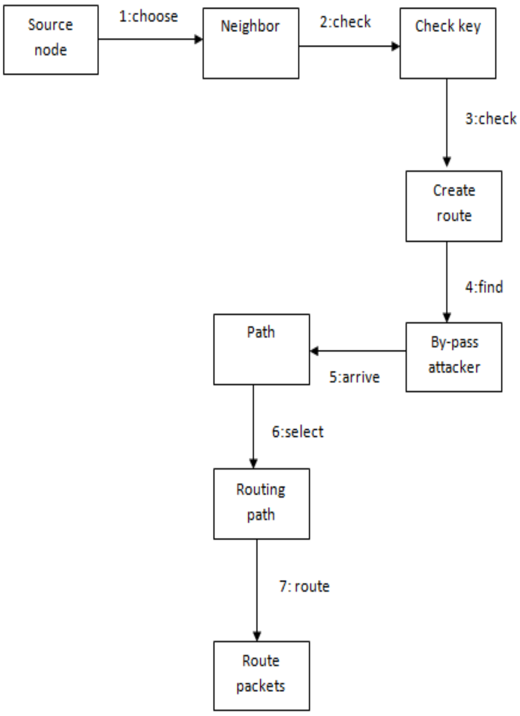


Figure 5. Process flow

The above Figure 5 represents collaboration diagram, it represent the process flow and its function. Assigning trust parameter, calculating fitness function and route selection are the sequence of process handled. It clear cut the process involved in the proposed work were the source node choose the neighbor node and check the key and it creates the routes path for sending the packets and also find the By-pass attacker which arrive in the path. thus the algorithms involved will avoid the attackers in the path and find the best routing path for allowing the route packets. Minimal configuration and quick deployment make ad hoc networks suitable for emergencies in military or natural disasters conflicts. The applications can further classify wireless Ad-hoc networks into Vehicular Ad hoc Networks, Mobile Ad hoc Networks, Smartphone Ad-hoc Networks, Wireless mesh networks and so on.

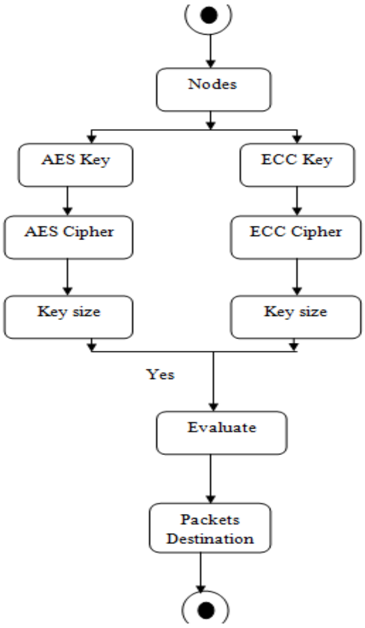


Figure 6. Activity diagram

The above Figure 6 show the activity diagram of the proposed system, where we represented the identified activities and its functional flow. The selected node will check the AES key and ECC key. At the next step it check for AES cipher and ECC cipher for evaluating the key size and send the packets to the destinations [9]. The modules included in our implementation are as follows Network model, AES implementation, ECC implementation, Key size Evaluation.

3.1 Network model

Consider a wireless sensor network consisting of sensor nodes that are uniformly and randomly scattered in a circular network; the network radius is R, with nodal density p, and nodes do not move after being deployed. Upon detection of an event, a sensor node will generate messages, and those messages must be sent to the sink node. Consider that link-level security has been established through a common cryptography-based protocol. Thus, consider a link key to be safe unless the adversary physically compromises either side of the link [10].

3.2 AES implementation

AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key longer keys need more rounds to complete. To decrypt an AES-encrypted ciphertext, it is necessary to undo each stage of the encryption operation in the reverse order in which it is applied [11].

3.3 ECC implementation

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage.

3.4 Key generation

Key generation is an important part where an algorithm should generate both public key and private key. The sender will be encrypting the message with receiver’s public key and the receiver will decrypt its private key. Now, select a number, d within the range of n. Generate the public key using the following equation,

$$Q= d * P \qquad (1)$$

Where d = the random number selected within the range of (1 to n-1). P is the point on the curve, Q is the public key and d is the private key.

3.5 Encryption

Let ‘M’ be the message that has to be sent. Consider ‘M’ has the point ‘P’ on the curve ‘E’. Randomly select ‘k’ from [1 - (n-1)]. Cipher texts will be generated let C.

$$C = M + (k * P) \qquad (2)$$

3.6 Decryption

Use the following equation to get back the original message ‘M’ that was sent.

$$M = C - d *(k*P) \qquad (3)$$

M is the original message that was sent.

3.7 Key size implementation

The key are uniquely generated and assigned for all nodes in the network and used for encryption. The cipher text generated with the key. The keys generated for nodes using AES and ECC are stored in a text files. The size of key are compared. ECC's main advantage is that you can use smaller keys for the same level of security, especially at high levels of security. The implementation shows that the Key size of ECC is very small compared to AES.

4. RESULTS AND DISSCUSION

Cryptographic schemes employ large keys and many rounds in their design for protection against malicious attacks. Wireless ad-hoc network thus requires adequate security-ensuring approaches that consume less power and show high performance. However, providing these requirements in one design is an impossible task because. Thus, developing a lightweight cryptographic algorithm is critical because the cryptographer must address security-performance, security-cost, performance-cost. In the proposed system, we used highly secure algorithm and also we can by-pass the attacker node. After finishing the development of any computer based system the next complicated time consuming process is system testing. During the time of testing only the development company can know that, how far the user requirements have been met out, and so on. Software testing is an important element of the software quality assurance and represents the ultimate review of specification, design and coding. The increasing feasibility of software as a system and the cost associated with the software failures are motivated forces for well-planned through testing.

- Source code testing
- Specification testing
- Module level testing
- Unit testing
- Integration testing
- Validation testing
- Performance testing
- Black box testing

- Output testing
- User acceptance testing

Table 1. Unit testing - test cases

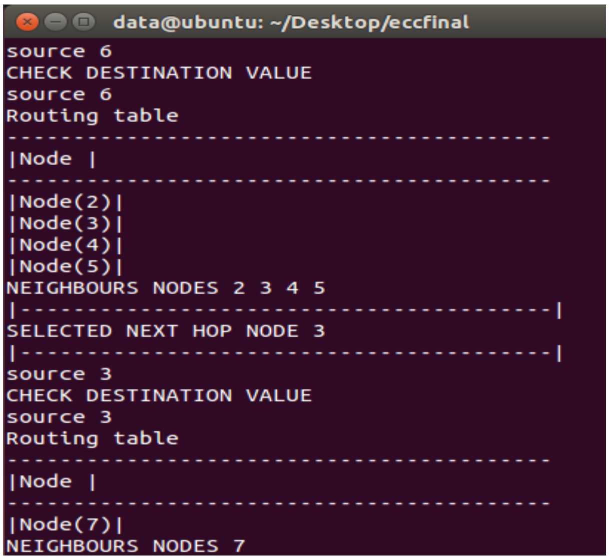
S. NO	Test Description	Test Procedure	Test Input	Expected Result	Actual Result
1	To check routing table	Input nodes ids	Execute robust.tcl	Nodes are created and deployed	Routing table is created
2	To check path creation	Input source and destination	Execute robust.tcl	Routes are created	Routing table is created
3	To check authentication	Input Key of Source node	Execute robust.tcl	Node Key values are checked	Node is authentic with true flag
4	To check packet delivery	Input Packets from Source node	Execute robust.tcl	Nodes should get packets delivered	Nodes received packets and monitored by sink for packet evaluations

Table 2: System specification

Parameters	Values
Processor	Intel(R) Core(TM) i3 -32227U CPU @1.90GHz
RAM	4 GB
Diskspace	255GB
Operating system	Windows 10
Application Software	Win2000/XP / Linux 9.0 VM ware Workstation

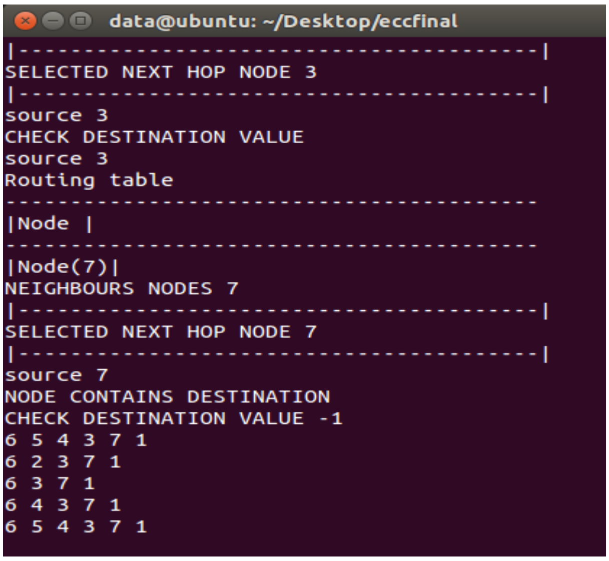
The simulation is carried out in ns-aallinone-2.34 with 33 number of nodes initialized in wireless network and routing is done is AODV protocol. The nam animator size is set at 1000 X1000 and neighbor nodes are detected with the distance <250. Nodes are assigned with AES and ECC keys for secure network.

The comparison of key size between AES algorithm and ECC algorithm, and it clearly indicates that the key size of ECC algorithm is very less compared to AES key size. The network communication cost can be reduced with ECC implementation. The key are uniquely generated and assigned for all nodes in the network and used for encryption. The cipher text generated with the key. The keys generated for nodes using AES and ECC are stored in a text files. The size of key are compared. ECC's main advantage is that you can use smaller keys for the same level of security, especially at high levels of security. The implementation shows that the Key size of ECC is very small compared to AES.



```
source 6
CHECK DESTINATION VALUE
source 6
Routing table
-----------------------------------------
|Node |
-----------------------------------------
|Node(2)|
|Node(3)|
|Node(4)|
|Node(5)|
NEIGHBOURS NODES 2 3 4 5
|----------------------------------------|
SELECTED NEXT HOP NODE 3
|----------------------------------------|
source 3
CHECK DESTINATION VALUE
source 3
Routing table
-----------------------------------------
|Node |
-----------------------------------------
|Node(7)|
NEIGHBOURS NODES 7
```

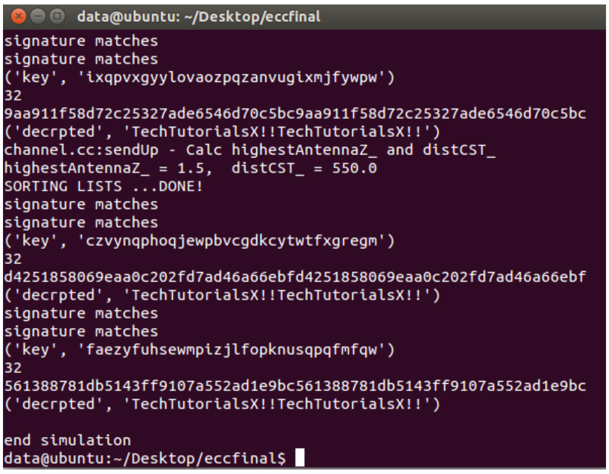
Figure 7. Routing path creation



```
|----------------------------------------|
SELECTED NEXT HOP NODE 3
|----------------------------------------|
source 3
CHECK DESTINATION VALUE
source 3
Routing table
-----------------------------------------
|Node |
-----------------------------------------
|Node(7)|
NEIGHBOURS NODES 7
|----------------------------------------|
SELECTED NEXT HOP NODE 7
|----------------------------------------|
source 7
NODE CONTAINS DESTINATION
CHECK DESTINATION VALUE -1
6 5 4 3 7 1
6 2 3 7 1
6 3 7 1
6 4 3 7 1
6 5 4 3 7 1
```

Figure 8. List of available paths

The Figure 7 and 8 shows the routing path and list of available paths which is based on the neighboring node detection table and it finds the best path and next hop node. The selected source node contains destination and check the destination values. In RSDA, AREQ is appended with the RREQ packet to accumulate the transmission rate value. The selective drop attack can be identified by checking the difference of a node with 2-hop neighbors and the nodes threshold value. The keys generated for nodes using AES and ECC are stored in a text files. The size of key are compared. ECC's main advantage is that you can use smaller keys for the same level of security, especially at high levels of security. The node notices an extreme variance, then the link will be disjointed from its parent as defective or malicious and takes up the responsibility for searching a new route to the destination.



```
signature matches
signature matches
('key', 'ixqpvxgyylovaozpqzanvugixmjfywpw')
32
9aa911f58d72c25327ade6546d70c5bc9aa911f58d72c25327ade6546d70c5bc
('decrpted', 'TechTutorialsX!!TechTutorialsX!!')
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
signature matches
signature matches
('key', 'czvynqphoqjewpbvcgdkcytwtfxgregm')
32
d4251858069eaa0c202fd7ad46a66ebfd4251858069eaa0c202fd7ad46a66ebf
('decrpted', 'TechTutorialsX!!TechTutorialsX!!')
signature matches
signature matches
('key', 'faezyfuhsewmpizjlfopknusqpqfmfqw')
32
561388781db5143ff9107a552ad1e9bc561388781db5143ff9107a552ad1e9bc
('decrpted', 'TechTutorialsX!!TechTutorialsX!!')

end simulation
data@ubuntu:~/Desktop/eccfinal$ 
```

Figure 9. ECC and AES signature checking in the message transmission

In Figure 9 the ECC and AES signature checking is done in message transmission were the key size is compared and then the signature should matches the key size and avoid the selective drop attack during the transmission of the message to the receiver. Thus the simulation process end by delivering the packets without any loss in the packets due to selective drop in the packet transmission.

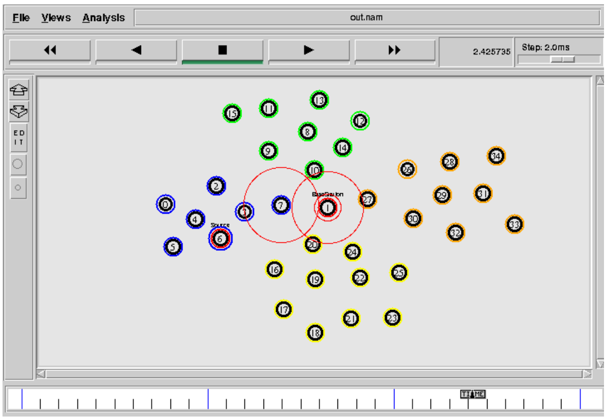


Figure 10. packet sending in nam animator

The network throughput, packet loss and end to end delay are registered and plotted below. The below graph defines the delay in the simulation phase. X axis time in (seconds) and Y axis delay time in (milliseconds). The experiment was running 5 seconds of time. End to End Delay refers to the time taken for a packet to be transmitted across a network from source to destination during the simulation time.

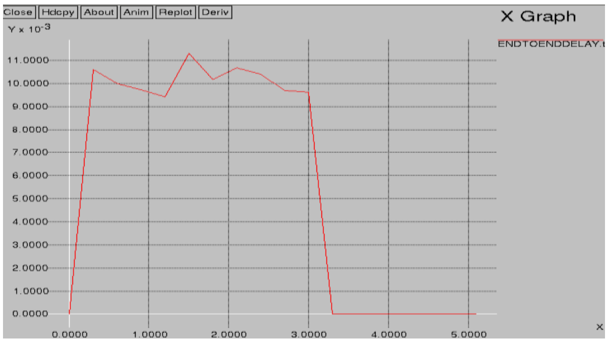


Figure 11. End to End Delay analysis

End-to-end encryption is a system of communication where only the communicating users can read the messages. It is necessary to calculate the execution time in order to evaluate the efficiency of the algorithm. The specific feature is communicating with the each nodes of the network rather than communicating with the intermediary node that exist to establish the network.

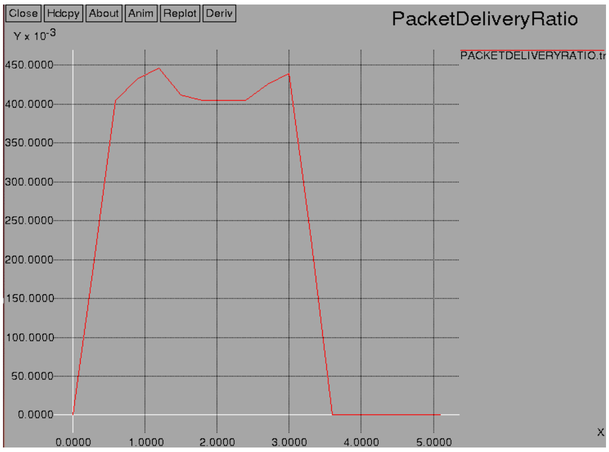


Figure 12. Throughput Analysis

The above graph defines the throughput for the proposed protocol. X axis time in (seconds) and Y axis throughput (bit/s) The experiment was running 5 seconds of time. Throughput is the rate at which a network sends receives data. It is a good channel capacity of net connections and rated in terms bits per second (bit/s). Throughput is the rate of successful message delivery over a communication channel by using the algorithms and to resist the selective drop attack in wireless ad hoc network.

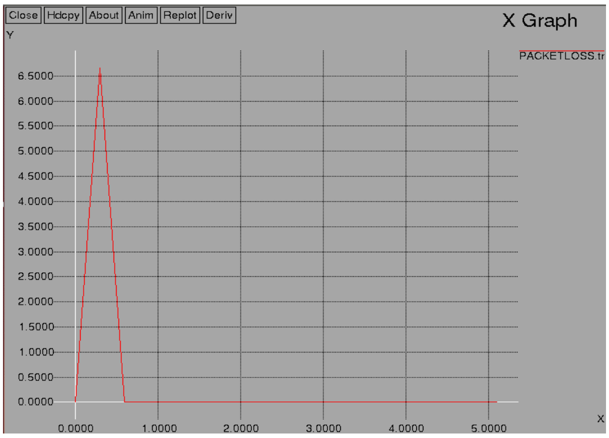


Figure 13. Packet loss analysis

The above graph defines the packet loss for the proposed protocol. X axis time in (seconds) and Y axis shows packet loss. The experiment was running 5 seconds of time. Packet loss is the number of packets lost at which a network sends receives data. Packet loss is responsible for many of the network issues especially in WAN connectivity and WiFi networks. The result from the above graph is that reason behind it like the issue is due to network connectivity or the quality of the network degrades due to TCP or UDP packet loss. This packet loss may happen if a router is receiving more data than it transmit or it forgot packets.

Table 3: Simulation parameter

Parameter	Values
Simulator	ns-2
Simulation Area	1000x1000m
Mobile Nodes	33
Node Speed	20 m/s
Packet Size	64 byte
Rate of Transmission of Packets	4 Packets per Second
Routing Protocols	AODV
Security Algorithms	AES, ECC
Simulation Time	5 seconds

The reserved bits in RREQ and RREP packets are used for analyzing the total number of packets sent by the source node and the destination node verifies the same. AREQ and Authenticated Route Reply (AREP) packets are used for checking the transmission rate. ECDSA based authentication code is attached with the message to mitigate from tampering of messages. In RSDA, AREQ is appended with the RREQ packet to accumulate the transmission rate value. The selective drop attack can be identified by checking the difference of a node with 2-hop neighbors and the nodes threshold value.

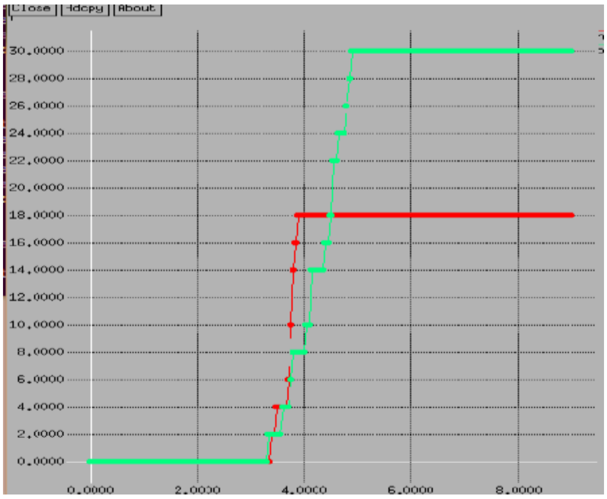


Figure 14. comparison of packet loss with and without RSDA

If the transmission rate is increased or decreased extensively, then the data transmission advances towards the destination, each node checks the weight of the link. If the variation between the last rate in AREQ and the node's estimated value is greater than the threshold value, then it is proven that at least one malicious node exists between nodes and the node is the one which added its last rate to AREQ. If the node notices an extreme variance, then the link will be disjointed from its parent as defective or malicious and takes up the responsibility for searching a new route to the destination.

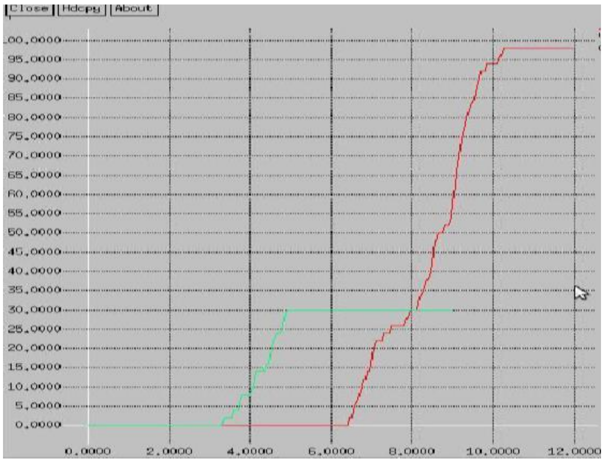


Figure 15. Comparison of Throughput with and without RSDA

The above graphs shows the comparison of Packet loss and Throughput based on AODV existing and proposed algorithms, X axis shows the time in seconds and Y axis shows the packet loss and throughput. that shows the result of with and without Selective drop attack. Fig 15 shows that packet loss is decreased without attack and increased with attack in AODV using ECC algorithm. Red line shows that packet loss is reduced with RSDA and green line indicates that packet loss is increased without RSDA.

In Figure 15 The network throughput is more without attack and network throughput is reduced due to selective packet drop attack in the network which is triggered by the malicious node. Red line indicates that with RSDA throughput is increased and green line indicates the reduced throughput without RSDA.

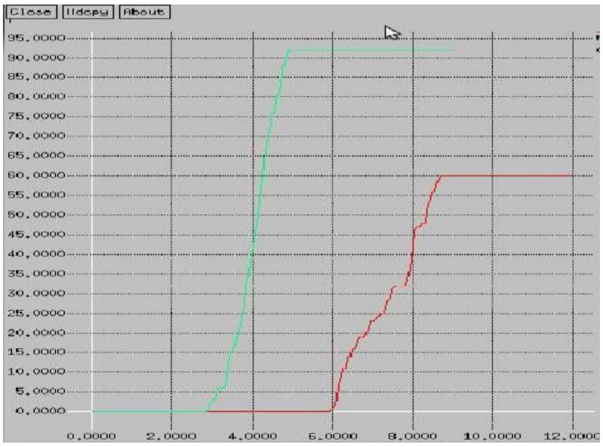


Figure 16. Comparison of end to end delay with and without RSDA

The above graph shows that end to end delay is more with attack and reduced without attack using AODV protocol in ECC algorithm. Thus the comparison is done based on with and without Resistive selective drop attack in wireless ad hoc network using AODV protocol by proposing the ECC algorithm.

Table 4: Comparison parameters of with and without RSDA

Sr. No.	Parameters	Without RSDA	With RDSA
1	End to End Delay	92 ms	60 ms
2	Packet Loss	30	18
3	Throughput	30 bits/s	95 bits/s

There is increased through put, reduced delay of packets and packet loss during the Selective Packet Forward Attack. It can be said that the proposed technique is better as compared to the existing technique. There are various techniques to isolate and prevent selective packet drop attack which degrade the system performance by decreasing throughput, increasing latency and end-to-end delay. In proposed technique delay, packet loss and throughput are better.

5. CONCLUSION AND FUTURE WORK

Novelty in the proposed methodology is implementation of elliptical curve cryptography. ECC key is well suited for wireless applications with smaller key size providing secure robust protection for wireless Ad-hoc network. Highly secure algorithm like AES and ECC is used and also can by-pass the attacker node. Using Wireshark the duplicate packets are analyzed and attack detection is identified. The network throughput, packet loss and end to end delay are analyzed and performance Comparison of with and without RSDA is analyzed. Proposed methodology shows improvement in reduction of selective drop attack. Minimal configuration and quick deployment make ad hoc networks suitable for emergencies in military or natural disasters conflicts. The applications can further classify wireless Ad-hoc networks into Vehicular Ad hoc Networks, Mobile Ad hoc Networks, Smartphone Ad-hoc Networks, and Wireless mesh networks.

In proposed work, the keys for encryption are generated using AES algorithm and ECC algorithm. Thus using AODV in wireless Ad-hoc network packet loss, throughput, end to end delay is analyzed. Comparison of with and without Resistive selective drop attack is analyzed. In future, the work can be extended to implementing few more key generation algorithm.

6. REFERENCES

[1] R. N. Ode, D. Perdana, and R. F. Sari, ‘‘Performance evaluation of AODV, AODV-UU, and AODV with malicious attack mode on vehicular ad-hoc network,’’ Adv. Sci. Lett., vol. 23, no. 5, pp. 3990–3994, 2019.

[2] A. Ranjan, V. Kuthadi, T. Marwala, and R. Selvaraj, ‘‘Swarm based archi- tecture for defense against stealthy attacks in mobile ad hoc network,’’ Ad Hoc Sensor Wireless Netw., vol. 36, nos. 1–4, pp. 107–126, 2020

[3] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, ``Wireless ad hoc networks," Encycl. Telecommun., vol. 1, no. 1, pp. 1-28, Dec. 2018.

[4] S. Youse, M. S. Mousavi, and M. Fathy, ``Vehicular ad hoc networks (VANETs): Challenges and perspectives," in Proc. 6th Int. Conf. Telecom-mun., 2006, pp. 761-766.

[5] H. Deng, W. Li, and D. P. Agrawal, ``Routing security in wireless ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70-75, Oct. 2019.

[6] I. F. Akyildiz, X. Wang, and W. Wang, ``Wireless mesh networks: A survey," Comput. Netw., vol. 47, no. 4, pp. 445-487, 2017.

[7] V. Balakrishnan and V. Varadharajan, ``Packet drop attack: A serious threat to operational mobile ad hoc networks," in Proc. Int. Conf. Netw. Commun. Syst. (NCS), Krabi, Thailand, 2016, pp. 89-95.

[8] M. Peng,W. Shi, J.-P. Corriveau, R. Pazzi, andY.Wang, ``Black hole search in computer networks: State-of-the-art, challenges and future directions," J. Parallel Distrib. Comput., vol. 88, pp. 1-15, Feb. 2016.

[9] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, ``Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," IEEE Syst. J., vol. 9, no. 1, pp. 65-75, Mar. 2015.

[10] A. Aijaz and A. H. Aghvami, ``Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective," IEEE Inter-net Things J., vol. 2, no. 2, pp. 103-112, Apr. 2015.

[11] P. Chen, S. Cheng, and K. Chen, ``Information fusion to defend intentional attack in Internet of Things," IEEE Internet Things J., vol. 1, no. 4, pp. 337-348, Aug. 2014.

[12] X. Meng and T. Chen, ``Event-driven communication for sampled-data control systems," in Proc. Amer. Control Conf. (ACC), vol. 1, 2013, pp. 3002-3007.

[13] Changhoon Yoon, Seungsoo Lee, Heedo Kang, Taejune Park, ‘FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks’, IEEE/ACM transactions on networking, VOL. 25, NO. 6,DEC 2017.

[14] A. K. Khare, J. L. Rana, and R. C. Jain, ‘‘Detection of wormhole, blackhole and DDOS attack in MANET using trust estimation under fuzzy logic methodology,’’ Int. J. Comput. Netw. Inf. Secur., vol. 9, no. 7, p. 29, 2017.

[15] C. Karlof and D. Wagner, ‘‘Secure routing in wireless sensor networks: Attacks and countermeasures,’’ Ad hoc Netw., vol. 1, no. 2, pp. 293–315, 2018.

[16] A. Nadeem and M. P. Howarth, ‘‘An intrusion detection & adaptive response mechanism for MANETs,’’ Ad Hoc Netw., vol. 13, pp. 368–380, Feb. 2014.

[17] D. Johnson, A. Menezes, and S. Vanstone, ‘‘The elliptic curve digital signature algorithm (ECDSA),’’ Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, Aug. 2019.

[18] D. Zhong, H. Lv, J. Han, and Q. Wei, ‘‘A practical application combining wireless sensor networks and Internet of Things: Safety management system for tower crane groups,’’ Sensors, vol. 14, no. 8, pp. 13794–13814, 2016.

[19] C. Perkins, E. Belding-Royer, and S. Das, Ad Hoc on-Demand Distance Vector (AODV) Routing, document RFC 3561, Nokia Research Center,IETF, 2018.

[20] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, ‘‘A dynamic anomaly detection scheme for

AODV-based mobile ad hoc networks,'' IEEE Trans. Veh. Technol., vol. 58, no. 5, pp. 2471–2481, Jun. 2017.

[21] J. Von Mulert, I. Welch, and W. K. G. Seah, ''Security threats and solutions in MANETs: A case study using AODV and SAODV,'' J. Netw. Comput. Appl., vol. 35, no. 4,

[22] S. Krco and M. Dupcinov, ''Improved neighbor detection algorithm for AODV routing protocol,'' IEEE Commun. Lett., vol. 7, no. 12, pp. 584–586, Dec. 2015.

[23] R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, ''A secure protocol for spontaneous wireless ad hoc networks creation,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 4, pp. 629–641, Apr. 2014.

[24] R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, ''Two secure and energy- saving spontaneous ad-hoc protocol for wireless mesh client networks,'' J. Netw. Comput. Appl., vol. 34, no. 2, pp. 492–505, 2013.

[25] S. Khan and J. Lloret-Mauri, Security for Multihop Wireless Networks.Boca Raton, FL, USA: CRC Press, 2014.