An Efficient Approach for the Security Threats on Data Centers in IOT Environment

Fahad H. Alshammari
College of Computing and Information Technology
Shaqra University, KSA

***Abstract*—Internet of Things has progressed from the conjunction of wireless knowledge, MEMS which is termed as micro electromechanical systems, micro facilities and the Internet. The conjunction has helped scratch down the storage walls concerning operating technology (OT) and information technology (IT), and allowing amorphous machine created data to be examined for understandings that will drive enhancements. The Things known as IOT is an arrangement of interconnected computing procedures, mechanical and digital machineries, substances or matters that are delivered with inimitable identifiers, and the ability to handover data over a system without necessitating human to humanoid, or human to computer collaboration. However, the security is one of the main concerns in Internet of things, which should be minimized. There are unnecessary requests from the attacker to overload the data center, which results in the hanging of the servers, decreasing the throughput, and requesting a transmission to the Data centers. This paper deals with an efficient approach to decrease the unwanted request at the Data Centers, so that the sessions will be reduced, and the unnecessary load will be reduced on the data centers, in order to mitigate the effect of attack as much as possible.**

***Keywords*—Internet of Things; Data centers; sessions; Security Threats; Networks**

I. INTRODUCTION

The complete Internet of Things framework will comprise of billions of entities, distinct devices, and amenities that can interrelate to exchange facts, and figures. Due to rapid progressions in mobile communication field, mobile Ad-hoc networks (MANET) and Radio Frequency Identification (RFID) modernization and apparatuses in IoT can hypothetically cooperate with one another anytime, anywhere and in any form[1][2]. The main target of Internet of Things is the development of smart surroundings and embarrassed independent devices for example smart conveyance, smart substances, smart metropolises, smart fitness, smart living. In business trends, Internet of things signifies tremendous outlook for dissimilar types of administrations which also includes IoT requests and service breadwinners, IoT policy providers, telecom machinists and software merchants.[4][5][6]. According to some approximations, over thirty billion associated things with extra 200 billion recurrent connections will produce around 714 billion in income proceedings by 2020. Many upright sections are predictable to knowledge a double digit evolution in upcoming centuries. The most forthcoming vertical solicitation provinces are consumer electronics, automotive productions, healthcare and intelligent constructions and conveniences [7][8][9].

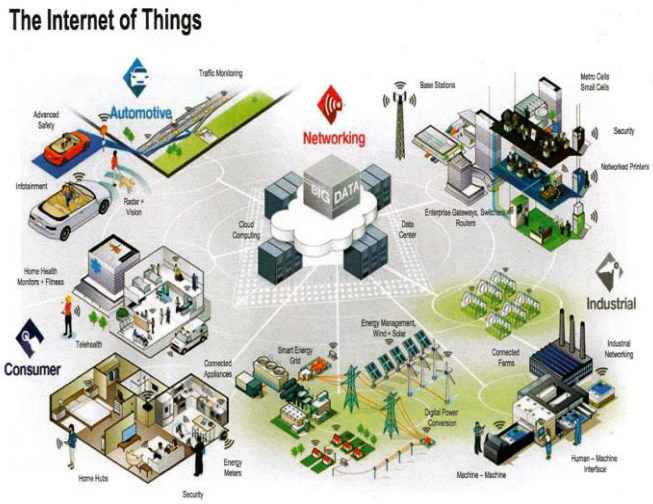

Fig. 1. Smart living criterion [http://www.mbuguanjihia.com/business/smart-living-understated-benefits-internet-things.html]

Some few examples related to the Internet of Things.

1) Heart Monitoring System
2) Smart mobile technology
3) Technology related to the wearable devices
4) Smart fabrication
5) Real time thermostat wireless systems.
6) Monitoring exercises
7) Smart Lightening System

The Internet of Things demonstrates a network deals with the physical objects that link to each other using internet. The objects and other valuable things can handover information wirelessly instead of any human efforts [10] [11] [12]

II. APPLICATION OF INTERNET OF THINGS

1) Parking in Smart Manner

It will help in the parking of vehicles in the appropriate manner so that it will manage efficiently in an organized manner through wireless systems.

2) Operational Health Structure

The IOT trends help in monitoring of vibrations and material conditions in building, bridges and different constructive areas.

3) **Detection of Smart Phones**

Detection of various devices based on Android and IOS operating systems in smart manner, which will also helpful in dealing with various theft cases.

4) **Filed levels based on Electromagnets**

The internet of things scenarios is very helpful in measuring the radiations which consists of electromagnetics signals from the Wi-Fi routers and cell base stations for high telecommunication applications.

5) **Smart transport infrastructure**

The IOT held devices is able to monitor the transport infrastructure and pedestrian intensities to enhance driving and mobile routes

6) **Managing Waste Materials**

Recognition of rubbish heights in vessels to optimize the garbage collection courses [13][14][15].

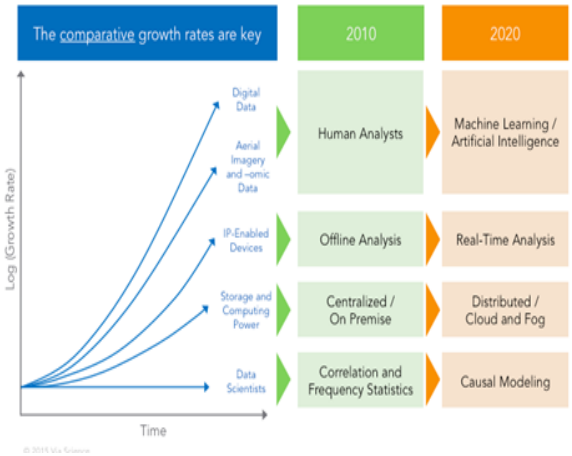

Fig. 2. The Increasing Trend of Internet of Things [http://www.viascience.com/meta-trends-iot/]

The figure2 mentions a glance about the growing rate of internet enabled devices. The development of Internet Protocol based enabled strategies means that extra scrutiny needs to transpire in real time scenario.

The IOT technology moving at the rate where statistics about individuals took period to transform and consequently analysis occurred over day by day. The quantity of loading space obtainable is also rising nonetheless at the similar rate as the quantity of data being produced by IP based devices. The number of associated strategies in the world is set to produce from 20 billion to 80 billion in the following five years. Storage planetary is now flowing to a more dispersed cloud contribution [16][17][18].

III. Security Threats in Internet of Things

As in Internet of Things moat of the attacks are determined and embattled where challengers use manifold trajectories of security threats to increase traction in the network from which is to be controlled as much as possible. In this atmosphere network executives cannot control the security approaches in which they merely get rid of the low hanging fruit of security vulnerabilities hoping that attackers would quickly move on to the next easy target [19] [20]

1) **Intruder Attack:** This type of attack is generally made on assumption. An intruder which is result the system and which can interrupt all communication ever communicated among IoT strategies and centers. The intruder is enormously accomplished and can even exceed the National Security Agency. But its aptitudes are slightly improbable. Attacks only get healthier, they not ever get inferior. Therefore, protection will be plentiful tougher if Internet of Things arrangement is considered to be intruder resistant. [21][22]

2) **Denial of service:** This type of dangerous attack is an effort to create a machine or resource inaccessible to its valuable users. The mainstream of strategies in Internet of Things is susceptible to supply occurrences because of low memory skills and limited reckoning possessions. The majority of security machineries involves high computational processes, and is afterward not appropriate for resource controlled IoT. Since in Internet of Things these attacks can occasionally deals with very costly behavior, investigators have to deal with extraordinary preparation to discriminate diverse types of alike attacks, also efficient policies to protect against them. The number of DoS attacks are in majority that may be hurled in contradiction of the IoT, example channels jamming process, high computational consumption possessions like recollection process, bandwidth, disk storage or processing time, and disruption of node information behavior.[23][24][25]

3) **Physical attacks:** These attacks interfere with hardware mechanisms. As the unattended and dispersed environment of IoT, most of the devices characteristically work in outdoor surroundings, which are extremely vulnerable to physical bouts.

4) **Attacks on privacy:** As the IoT makes huge capacities of info easily obtainable through distant access machineries; privacy fortification in IoT is becoming hard challenging criteria. The antagonist needs not to be actually present to transmit out investigation, but info gathering can be finished namelessly with very little risk [26][27][28].

TABLE. I. COMPONENTS OF SECURITY INFLUENCING SECURITY FUNCTIONALITY [29][30]

Component	Functionality of component	Goals of security
Authorization	Controlling and Accessibility	Data confidentiality and integration
Authentication	Authenticating user and devises	Authenticating accountability
Key management and exchanging	Cryptography process	Communication integration and confidentiality
Trust Management	Service levels and user density collection	Service trust and reputation

IV. LITERATURE REVIEW

Nima Bari, Ganapathy Mani, Simon Berkovich et al. [5] describes the new methodology for the internet of things in terms of science and quantum mechanics which shows that it will be the constructive approach for them to design any system which is based on internet. They have presented the synchronization process with less fault tolerance in cellular automation substructure. They have worked on holographic criteria which is very useful for the determination of all required characteristics of quantum mechanics.

Alfred Zimmermann, Rainer Schmidt, Kurt Sandkuhl, Matthias Wißotzki, Dierk Jugel, Michael Möhring et.al [6] related the real world with the internet of things which will relate today's numeral policies with troublemaking business functioning prototypes and fast varying marketplaces. As the trends are totally based on internet and due to the increasing diversity of this current technology, products administrations have to control and extend earlier Enterprise Architecture determinations to enable commercial value by assimilating Internet of Things planning. Both structural design manufacturing and information schemes management and commercial models are multifaceted and currently assimilating beside the IOT synergistic themes, like cloud computing services, semantic decision provision through physics methodology and knowledge derived systems, mobility and alliance systems.

Mohamed Abomhara,Geir M. Køien et.al [7] presents the real world security issues in internet of things. As Internet systems will be abundant and universal, there is lot of number of safety and confidentiality matters will rise. Reliable, inexpensive, well organized, and actual security and discretion, for Internet of things are obligatory to confirm exact and precise discretion, integrity, and substantiation among others. In this valuable paper, they have inserted the vision of IOT numerous security intimidations challenges in the area of IoT are presented. The existing state of investigation on IoT refuge supplies is deliberated, and future investigation guidelines with admiration to IoT refuge and discretion are presented in this paper.

Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan et.al [8] describes the analysis of security subjects and opens glitches in Internet of Things. As the deployments of the internet of things devices increases day by day, then there are a lot of chances of the malicious attacks to cooperation the sanctuary and confidentiality of the IoT strategies. Number of researchers has discovered various security trials; there is an unsuccessful lack of a methodical study of the refuge tests in the IoT. So in this paper they have gone thorough examination of IoT sanctuary experiments and difficulties. They present thorough analysis of attack exteriors, danger reproductions, sanctuary matters, necessities and contests. They also deliver exposed problems in IoT refuge and discretion to direct the courtesy of investigators into resolving the utmost dangerous difficulties.

Hui Zhu, Fen Liu, Hui Li et.al [9] presented an efficient approach as a framework for the security threats in Internet of Things for the location based scenarios. As the mobile technology is increasing day by day and the advancement of wireless communication skill, location constructed facilities have made human life more suitable, and they have provided polygons longitudinal interrogation, which is able to provide more flexible approach and consumes substantial interest freshly. The embellishment of polygons longitudinal query statically faces many experiments including the evidence privacy. In their approach, they have presented a well-organized and confidentiality conserving framework based location services called Polaris.

Problem statement deal with the security of the network, which is one of the main issue in Internet of Things. Therefore, there is no any bullet who can resolve the issue in IOT. The attacker can attack on IOT based products, and it will create a huge chance to drop the packets, which contains necessary information, and will decrease the lifetime of the network. As the amount of data being transferred is increasing due to number of increasing users, there is need of expanded bandwidth growth. The attack on Data center will increase the unwanted number of sessions, which will produce unnecessary loads on data center and halts the operation.

The proposed methodology deals with the mitigation of the attack scenario to decrease the vulnerability for the security of the network and will have high network lifetime.

V. PROPOSED METHODOLOGY

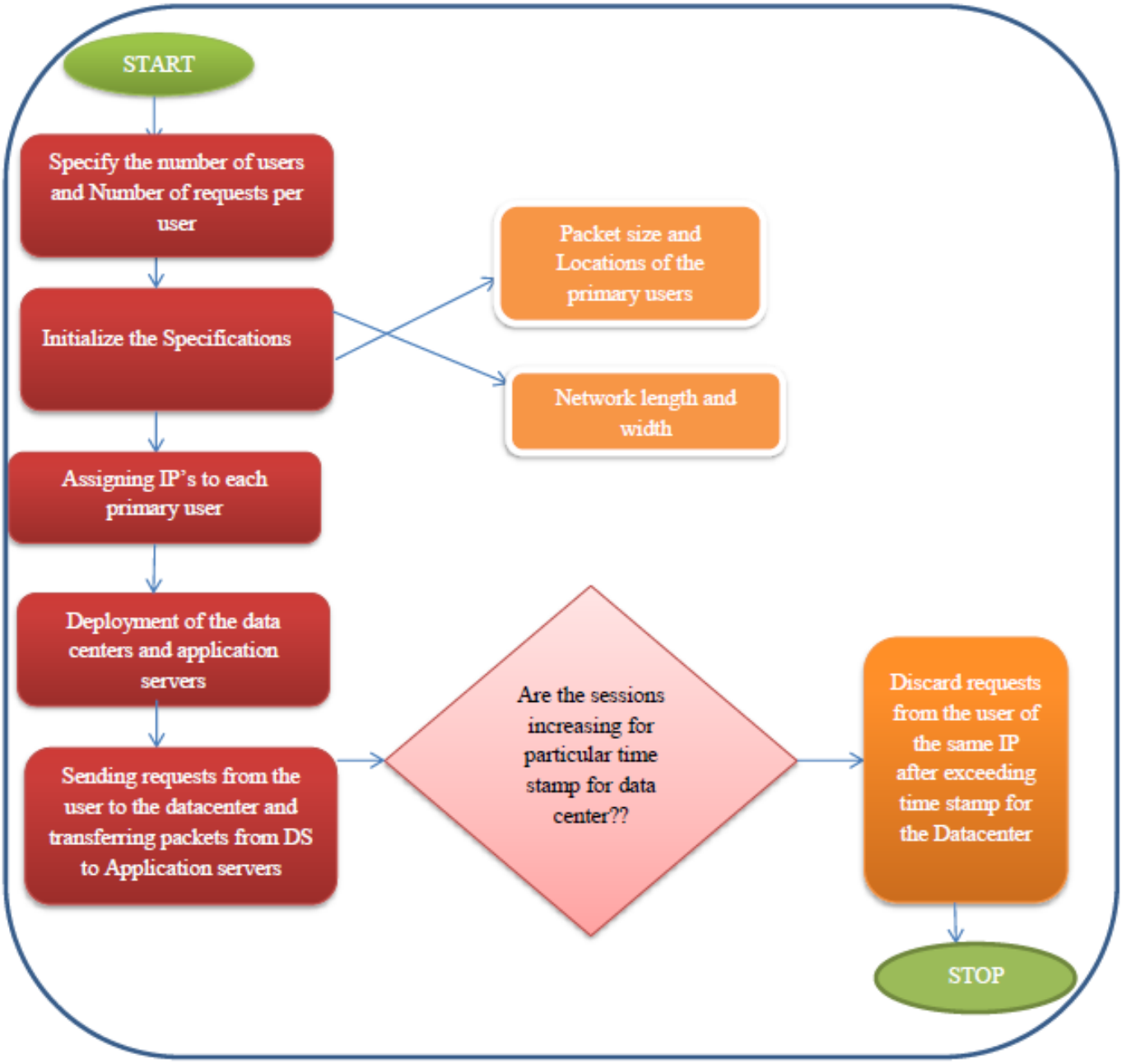

Fig. 3. Flow diagram of the proposed approach

```
1.  // Initialize the Specifications
2.   Initialize network length and network width
3.  Evaluate the Locations for the primary users
4.   For each primary user i do so
5.          Calculate x-locations and y-locations for the primary user
6.          Store the Id and their IP addresses for each user
7.   End
8.  Deployment of the data centers and Application servers for the execution of the requests
9.  // Initialize the Number of Sessions
10.  For each user i do
11.        If no_sessions > time_period for the execution of the Data center
12.             Load on the Data Center Increases
13.             Unnecessary Requests Increases and Suspect Occurs
14.        End
15.  End
16.  // Evaluation of the parameters in the presence of attacks
17.       Calculate the Ec, Td, Np
18.        Ec = Energy Consumption of the Data Center to execute the REQ
           Td = Time Delay to reach the Request of the user to the Data Center
           Np = Number of packets received
19.    Mitigate the Attack by excluding the requests coming from the same IP addresses after exceeding Tp for
   the   Data Centers for the execution of REQ
20.  // Evaluation of parameters after Applying proposed approach
21.       Calculate the Ec, Td, Np and compare it with the parameters in the presence of attack
```

Fig. 4. Pseudo code for the proposed Scenario

VI. Result and Analysis

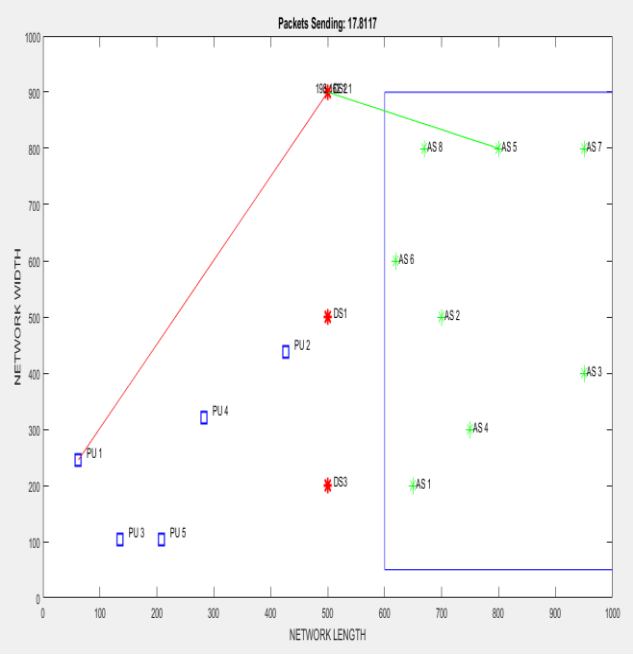

Fig. 5. Simulation scenarios for the proposed network

Figure 5 shows the simulated scenario of the proposed networks, which deals with the Primary users, Data Centers, Application servers, and shows the communication from the primary user to data centers. With the IP address in red color line and from green color to the Application servers in green color which deals with the execution of the requests from the primary users to the data centers.

$$\text{Energy Consumption} = (\sum xi * ds) * \sum V_i \quad (1)$$

Where

1) Xi is the energy consumed for the data center to be transmitted requests to the application servers.

2) Ds is the delay for the primary user for the request to be executed at the Data Center.

3) Vi is the total number of application servers responsible for the excitation of the number of requests.

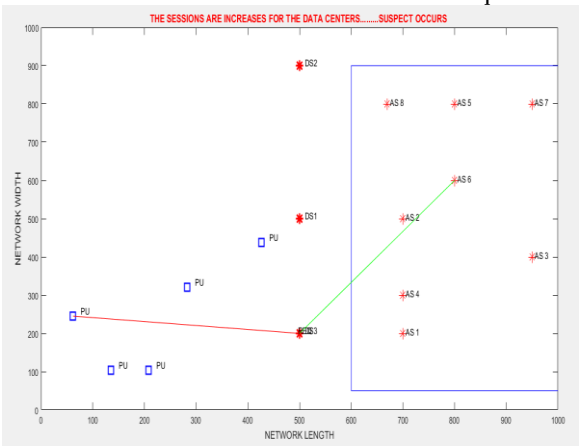

Fig. 6. Simulation for the attack scenario

Figure 6 shows the attack simulation with the increase of the number of sessions at the particular time for the data center, to receive the requests. As the number of sessions increase in the particular time, the receiving requests increase for the data center, then the suspect occurs and the indication of the attack will be found in the network.

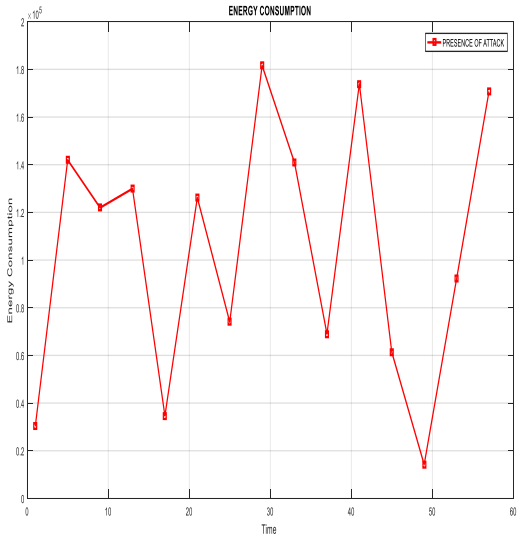

Fig. 7. Energy consumption (presence of attack)

From the figure 7, it is clear that the data center is consuming more energy in the presence of attack, which should be less for the appropriate working of execution of the requests from the primary users.

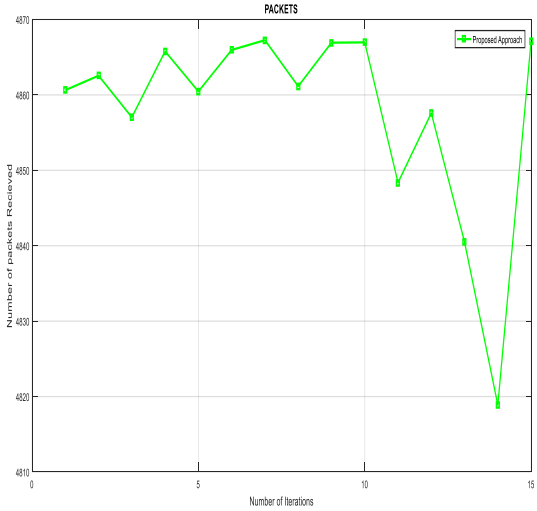

Fig. 8. Energy consumption (proposed approach)

Figure 8 shows the Energy consumption after mitigation of attack. Therefore, as a result of that, it appears that the proposed approach performs well, and helps to mitigate the effect of the attack.

$$\text{Number of Packets received} = \frac{(\sum xi * \sum ri)}{N} \quad (2)$$

Where

1) Xi is the energy consumed for the data center to be transmitted requests to the application servers.

2) Ri is the number of requests per user to be executed.

3) N is the total number of Primary users.

$$\text{Delay time} = \frac{(\sum Pi) * (\sum ri)}{N} \quad (3)$$

Where

1) Pi is the total number of packets received.

2) Ri is the number of requests per user to be executed.

3) N is the total number of Primary users.

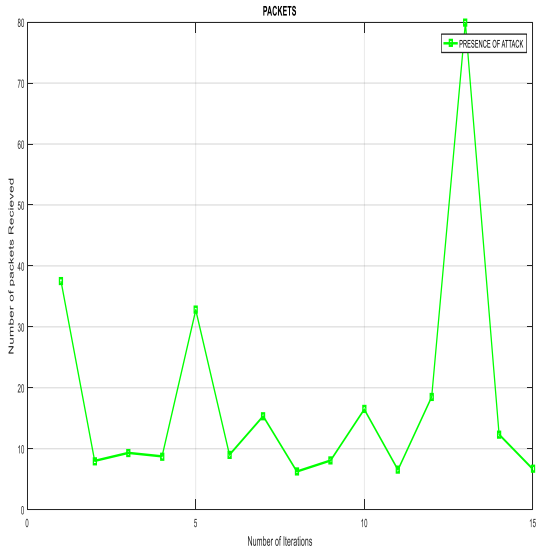

Fig. 9. Packets reception in presence of Attack

Figure 9 shows the packets reception rate in the presence of the attack. The number of packets should be received more to the data centers because more the number of packets will be received by the Data Centers, more will be the successful execution of the requests of the primary users.

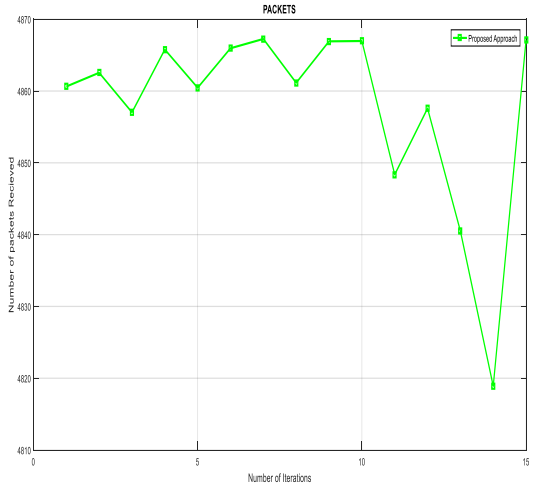

Fig. 10. Packets reception (proposed approach)

Figure 10 shows that the packets are successfully delivered, to complete the execution of the requests, as processed by the data center, and helps to low down the effect of the attack in IoT environment.

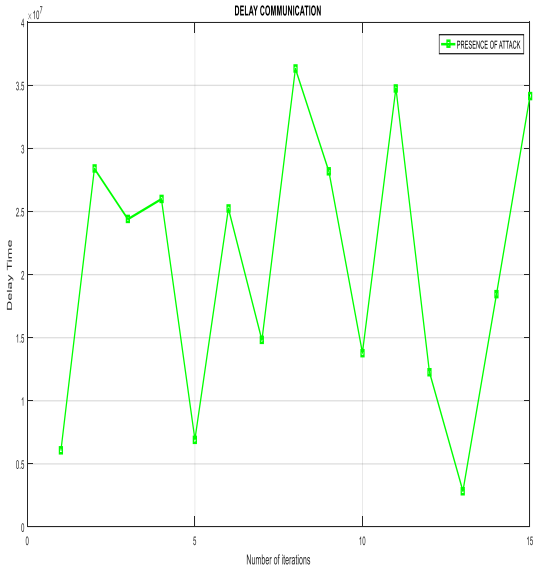

Fig. 11. Delay (presence of Attack)

Figure 11 shows the delay rate in the presence of the attack. Less number of packets is receiving with high delay, which decreases the execution of the network, and increases the response time of the network, which degrades the performance of the network.

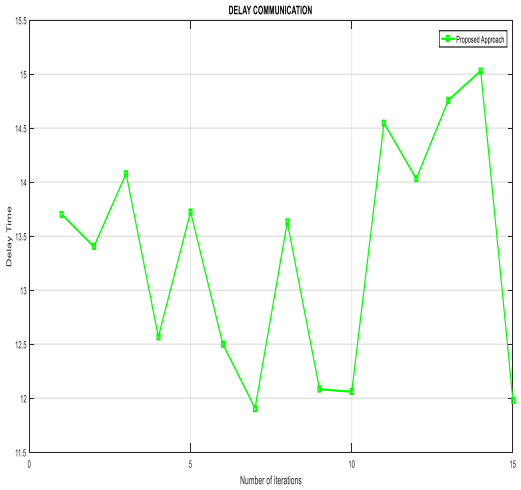

Fig. 12. Delays (Proposed Approach)

Figure 12 shows that Delay for the execution of the requests by the data center is less, which shows the less effect of the attack in the IoT environment, and deals in the high efficiency of the network by executing the probable requests, and rejecting the unnecessary requests at less delay time.

VII. Conclusion and Future Scope

As a rapid development of Internet things based applications in real world, the chances of the security threats are increasing in the IoT environments. Therefore, it should be diminished as much as possible up to great extent, and the proposed area of research deals with the same scenario to mitigate the effect of the attack environment, and shows the evaluation of attack on data centers, and their mitigations are diminishing for the same.

The future of this paper deals with such hybridization of the security algorithms, which deals with the efficient encryption of data, which will be sent to the data centers for the secure communications.

Acknowledgements

My deepest acknowledgements to the University of Shaqra for the support received during the preparation of this paper and that made possible its successful completion. Thank you for promoting this research, which is part of my growth as a professional and that in turn, such research will contribute to the overall knowledge of software engineering.

References

[1] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, pp. 1-8. IEEE, 2014.

[2] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17, no. 3 (2015): 1294-1312.

[3] Matharu, Gurpreet Singh, Priyanka Upadhyay, and Lalita Chaudhary. "The Internet of Things: Challenges & security issues." In Emerging Technologies (ICET), 2014 International Conference on, pp. 54-59. IEEE, 2014.

[4] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, pp. 1-8. IEEE, 2014.

[5] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, pp. 1-8. IEEE, 2014.

[6] Zimmermann, Alfred, Rainer Schmidt, Kurt Sandkuhl, Matthias Wißotzki, Dierk Jugel, and Michael Möhring. "Digital enterprise architecture-transformation for the Internet of Things." In 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, pp. 130-138. IEEE, 2015.

[7] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, pp. 1-8. IEEE, 2014.

[8] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things." In 2015 IEEE World Congress on Services, pp. 21-28. IEEE, 2015.

[9] Zhu, Hui, Fen Liu, and Hui Li. "Efficient and Privacy-preserving Polygons Spatial Query Framework for Location-based Services." (2012).

[10] Said, Omar. "Development of an innovative internet of things security system." Int. J. Comput. Sci. Issues (IJCSI) 10, no. 6 (2013): 155-161.

[11] Covington, Michael J., and Rush Carskadden. "Threat implications of the internet of things." In Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1-12. IEEE, 2013

[12] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things." In 2015 IEEE World Congress on Services, pp. 21-28. IEEE, 2015

[13] Aldossary, Alia A., and Akram M. Zeki. "Web User'Knowledge and Their Behavior towards Security Threats and Vulnerabilities." In 2015

4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), pp. 256-260. IEEE, 2015

[14] Lee, Yunjung, Yongjoon Park, and DoHyeun Kim. "Security Threats Analysis and Considerations for Internet of Things." In 2015 8th International Conference on Security Technology (SecTech), pp. 28-30. IEEE, 2015

[15] Liu, Caiming, Yan Zhang, Zhonghua Li, Jiandong Zhang, Hongying Qin, and Jinquan Zeng. "Dynamic Defense Architecture for the Security of the Internet of Things." In 2015 11th International Conference on Computational Intelligence and Security (CIS), pp. 390-393. IEEE, 2015.

[16] Malyuk, Anatoly, and Natalia Miloslavskaya. "Information Security Theory for the Future Internet." In Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, pp. 150-157. IEEE, 2015.

[17] Desnitsky, V. A., I. V. Kotenko, and S. B. Nogin. "Detection of anomalies in data for monitoring of security components in the internet of things." In Soft Computing and Measurements (SCM), 2015 XVIII International Conference on, pp. 189-192. IEEE, 2015.

[18] Shivraj, V. L., M. A. Rajan, Meena Singh, and P. Balamuralidhar. "One time password authentication scheme based on elliptic curves for internet of things (IoT)." In Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, pp. 1-6. IEEE, 2015.

[19] Zhang, Yuanyu, Yulong Shen, Hua Wang, Jianming Yong, and Xiaohong Jiang. "On Secure Wireless Communications for IoT Under Eavesdropper Collusion."

[20] Arış, Ahmet, Sema F. Oktuğ, and Sıddıka Berna Örs Yalçın. "Internet-of-Things security: Denial of service attacks." In 2015 23nd Signal Processing and Communications Applications Conference (SIU), pp. 903-906. IEEE, 2015.

[21] Chouhan, Pushpinder Kaur, Feng Yao, and Sakir Sezer. "Software as a service: Understanding security issues." In Science and Information Conference (SAI), 2015, pp. 162-170. IEEE, 2015.

[22] Głowacka, Joanna, Jaroslaw Krygier, and Marek Amanowicz. "A trust-based situation awareness system for military applications of the internet of things." In Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, pp. 490-495. IEEE, 2015.

[23] Habib, Kashif, and Wolfgang Leister. "Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures." In 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-5. IEEE, 2015.

[24] Jaballah, Wafa Ben, Mauro Conti, Mohamed Mosbah, and Claudio E. Palazzi. "Impact of security threats in vehicular alert messaging systems." In 2015 IEEE International Conference on Communication Workshop (ICCW), pp. 2627-2632. IEEE, 2015.

[25] Kumar, Malay, Jasraj Meena, Rahul Singh, and Manu Vardhan. "Data outsourcing: A threat to confidentiality, integrity, and availability." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1496-1501. IEEE, 2015.

[26] Lee, Kanghyo, Donghyun Kim, Dongsoo Ha, Ubaidullah Rajput, and Heekuck Oh. "On security and privacy issues of fog computing supported Internet of Things environment." In Network of the Future (NOF), 2015 6th International Conference on the, pp. 1-3. IEEE, 2015.

[27] Medjek, Faiza, Djamel Tandjaoui, Mohammed Riyadh Abdmeziem, and Nabil Djedjig. "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility." In Programming and Systems (ISPS), 2015 12th International Symposium on, pp. 1-9. IEEE, 2015.

[28] Atamli, Ahmad W., and Andrew Martin. "Threat-based security analysis for the internet of things." In Secure Internet of Things (SIoT), 2014 International Workshop on, pp. 35-43. IEEE, 2014.

[29] Li, Depeng, Zeyar Aung, John Williams, and Abel Sanchez. "P3: Privacy preservation protocol for automatic appliance control application in smart grid." IEEE Internet of Things Journal 1, no. 5 (2014): 414-429.

[30] Riahi, Arbia, Enrico Natalizio, Yacine Challal, Nathalie Mitton, and Antonio Iera. "A systemic and cognitive approach for IoT security." In Computing, Networking and Communications (ICNC), 2014 International Conference on, pp. 183-188. IEEE, 2014.