Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 1125-1139

http://www.ripublication.com

Architecture, Features and Security Concern of IoT

Rishi Kashyap[1], Palak Bansal[1], Suman Bharti[1*] and Aarti Malyan[1]
[1]Department of Electronics, Bhaskaracharya College of Applied Sciences, University of Delhi, India.

Abstract

Internet of Things is an emerging technology in which physical objects are made to communicate with each other smartly. Internet of Things (IoT) is a fast growing area, however, there are some concerns related to the security and privacy of the network. In this paper we give an overview of the various security issues and opportunities in IoT. Further, we give a comparative analysis of security in IoT and IPv6 followed by various algorithms and security frameworks for IoT. Further, it describes the security breaches possible within each layer, thereafter, imparting details about the various techniques and algorithms that can be incorporated within each layer in order to rectify the security problems.

Keywords: Blowfish Array, Internet of Things, Intrusion Detection System, IoT Architecture, RSA Algorithm.

1. INTRODUCTION

In this era of technology boom, we are rapidly moving toward the world of virtualization. A world where humans along with smart machines embraced by technologies like that of artificial intelligence According to a report by CISCO the population of IoT has already surpassed the population of humans in 2016. Recent trends in growth of IoT and smart devices show that by the year 2020 the IoT market may grow up to 50M connected devices. With such a promising growth IoT hold a pole position in research and industry [1].

This paper deals with the security features that have been incorporated at different

existing layers of Internet of Things and provides a review whether these technology guarding the security issues and concerns have been successful in their efforts or more attention is required in that particular layer.

2. IoT ARCHITECTURE

IoT Architecture comprises of all the minutiae details of the IoT process from sensing of the data for providing network interface to read data from database and then, providing it to user in an interactive manner. To reduce this complexity in architecture IoT has been segregated in 4 main layers. viz,

I. Perception Layer
II. Networking Layer
III. Middleware Layer

Application Layer and others play a pivotal role in creating architecture for a better world to live. Internet of Things is one such technology which plays a very crucial part in fulfilling the above challenges. The IoT is a revolution in this modern world; it is a paradigm where different computing systems are connected to each other along with the assistance of cloud architecture to create a giant interconnected framework that can be accessed by humans from any part of the world, thus pushing the idea of virtualization in modern day reality. In the coming years every device in this world will be supported by microcontrollers and transceivers for communicating with its periphery as well as humans. Although IoT serves as boon for the mankind by allowing us to transmit and receive data on our ease and making the world more friendly , the flip side of coin need to be taken care as well i.e. its security features, concerns and constraints. These all also require equal devotion.

The detail description of each layer has been discussed below.

Perception Layer(Sensing Layer) - The layer's main task is to collect data from user in real-time with the assistance of various sensors, namely RFID, Barcodes, QR codes or any other sensor and transfer it to above layer for processing this data. The sensor like RFID tags are incorporated on the devices and contain all the information about it, that can be scanned to receive all the data related to it. Once scanned data is transferred to above layer in hierarchy, i.e. networking layer, it is used to process the data accordingly.

Networking Layer- The network layer deals with transmission of data. The data received from the sensors in the sensing layer is further transmitted according to a particular processing system with the assistance of any networking protocol like Internet or any reliable networking layer. The data from sensing layer which was transferred to network layer by RFID tag can be transmitted to the database. Thw database is used for collection of data that RFID Tag or any sensor collects via

Internet or any intranetworking platform in which the sensor is working and is compatible. Once the data has been stored in the database through a processing system the higher level of hierarchy comes into play i.e. the middleware level.

Middleware Layer- This network layer is service-oriented and deals with the processing of information. It links the data to the particular database for storage of the collected data. The data of the sensors that has been transmitted from networking layer is used for storage and processing of information according to a particular algorithm.

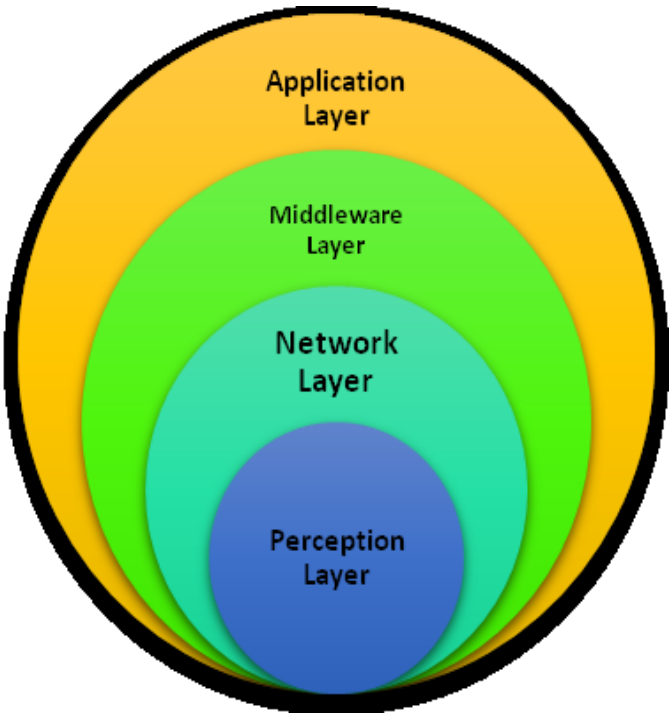

Figure 1: Layers of IoT_Architecture

Automated actions are taken every time the data is entered into the database. The data that has been transferred from the sensors like RFID via any communication medium using network layer is now processed and particular actions are taken according to corresponding data after they are fed into the database. After the information is processed and appropriate actions are taken, application layer comes into play where the practical application of the data is performed in real life time.

Application Layer (Interface Layer) - This layer deals with the users in real life time scenario. It is this layer where real application of the data takes place in real time. This layer provides interface to the user to use the facilities provided by Internet of Things in various smart devices, viz mart housing system, smart LED system, smart vehicles and many other applications.

The working of all the layers can be understood by the following example, let us consider a situation where the user has a smart LED system present in his home where the functionality of the smart LED is to control the brightness and somewhat control the color of LED, this is done with the help of sensor which continuously monitors the room temperature. Now when the temperature of the room decreases below certain level the sensor senses that data and sends the information, this is the functionality of the **perception layer**. The analog data that was transferred by the sensor is then converted in digital form and transferred to the system which handles the logistic of the data. The communication channel can be Bluetooth or a Wi-Fi or even a radio frequency. Transfer the information is the work of **Network layer**. As the data reaches the database it gets stored into it and according to the program fed into the device it concludes that temperature has decreased to a certain level and it needs to change the brightness of the LED. The processing of the information is the work of the **middleware layer**. Now this layer takes appropriate action according to the data that has been transmitted that is reducing or enhancing the brightness and changing of the color accordingly. At the **application layer,** the action for controlling of the brightness and color of the LED is performed and the user can see the change in brightness and color of the LED according to change in temperature. So this is how each and every layer of IoT works together in perfect synchronization with each other to provide us with suitable results.

3. SECURITY IN IoT

IoT has been a great leap in development of smart environment around us, be it smart cities, smart homes, smart cars or even smart devices. The role of IoT is the most dominant, as every part in the development of this giant framework directly or indirectly is connected to IoT. Although IoT has been the protagonist in this whole process but there are few aspects that need equal devotion in order to make this a much better experience for every individual. One of the most important aspects to enhance the quality of IoT is security of IoT framework. Although a significant work has been done in the area of IoT architecture and IoT framework protocols, but security of IoT devices has not been considered since the beginning. The basic security requirement of IoT is CIA (Confidentiality, Integrity and Availability) which can be easily compromised with the fact that IoT devices are small, easy to reach and not highly secured. IoT Architecture needs continuous updates keeping in mind the latest trends in security issues and threats like Hajime IoT worm which recently infected 3,00,000 devices, 8 DDoS attack in application layer, Teddy bear data breach, BrickerBot Malware attack which destroys unsecure IoT devices and many more needs to be mitigated [2][3][4][5]. In this section we present some literature on work related to IoT security as shown in table 1 given below.

Table 1: Literature summary of some important work done in IoT security.

AUTHOR	TITLE	YEAR	DESCRIPTION
Molnar D., and Wagner D.,	Privacy and Security in Library RFID: Issues, Practices and Architectures [6]	2004	RFID library related issues are exposed in this paper and simple schemes to ensure privacy are also proposed.
Mitrokotsa A., et. al	Classifying RFID attacks and defenses [7]	2010	This paper also deals with RFID security concerns and helps to categorize the various risks associated with RFID for better understanding of its security issues.
Hancke, G. P., et. al	Security challenges for user-oriented RFID applications within the 'Internet of Things' [8]	2010	The paper deals mainly with the RFID; it's role, how it assists the user based applications and extreme level security issues arising within them.
Weber R. H.,	Internet of Things - New security and privacy challenges [9]	2010	The paper talks about establishing an adequate legal framework that must be taken for the IoT and would best be established by an international legislator for the security of underlying technology.
Roman R., et. al	Securing the Internet of Things [10]	2011	The paper highlights the importance of IoT in present day scenario in creating a framework for enhancement of economy, but it also requires novel approaches to ensure its safe and ethical use. Various complexities associated with IoT such as data and privacy, identity management, fault tolerance, identity and ownership, etc. are discussed with fine details.
Khoo B.,	RFID as an Enabler of the Internet of Things: Issues of Security and Privacy [11]	2011	RFID stands among the enabling technology of IoT, With widespread of RFID in IoT application; it has given rise to serious issues including security and privacy concerns. This paper highlights RFID usages and conducts a threat analysis of RFID system components and providing us with solution to overcome the challenge.
Liu C., et. al	Research on Immunity-based Intrusion Detection Technology for the Internet of Things [12]	2011	An artificial immune system for the intrusion detection in IoT network is constructed in this paper.
Clarke J., et. al	Trust & security RTD in the internet of things: Opportunities for international cooperation [13]	2012	Authors of the paper writes about the research in the field of RTD (research and technological development), focusing Europe, dealing with privacy, security and trust associated with IoT.
Bhattasali T., et. al	Sleep Deprivation Attack Detection in Wireless	2012	This paper focuses on various forms of attack on the sensory nodes in WSN, among

	Sensor Network [14]		all of them it considers sleep deprivation attack to be the most dangerous one where the attacker reduces the lifetime of the sensor by increasing its battery drainage, and this paper develops a hierarchal framework to counter the above mentioned challenge.
Suo H., et. al	Security in the Internet of Things: A Review [15]	2012	This paper focuses on the security aspect of IoT by deep researching the progress of IoT, by studying their different architecture and features and discussing the research status of various key technologies like encryption mechanism, protecting sensor data, communication security and cryptographic algorithms, and outlining the challenges.
Mahalle P. N., et. al	Identity authentication and capability based access control (iacac) for the internet of things [16]	2013	The author proposed a novel, integrated approach of authentication and access control in IoT devices.
Qiang C., et. al	Research on Security Issues of the Internet of Things [17]	2013	This paper highlights existing researches of network security technologies of IoT and provides a newer approach for IoT applications and design.
Liu C., et. al	A novel approach to IoT security based on immunology [18]	2013	A dynamic approach to ensure security of IoT based on immunology along with simulation results are presented in this paper.
Zhao K., and Ge L.,	A survey on the internet of things security [19]	2013	This paper discusses the various security problems and their solutions arising within the different architectural layers of IoT, elaborating those that are associated with the perception layer.
Roman R., et. al	On the features and challenges of security and privacy in distributed internet of things [20]	2013	Distributed IoT is the main concern of this paper; thereby throwing light on its advantages, disadvantages, features, security and privacy.
Farooq et. M., et. al	A Critical Analysis on the Security Concerns of Internet of Things (IoT) [21]	2015	It defines the secured architecture of the IoT, also discussing different security issues and privacy concerns.
Mahmoud R., et. al	Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures [22]	2015	Focus of this paper is mainly on the security concerns of IoT, overviewing the challenges, the remedies to resolve them and future aspects to secure IoT.
Granjal J., et. al	Security for the Internet of Things: a survey of existing protocols and open research issues [23]	2015	The authour presented a survey that considers the existing tools and protocols to ensure security of communications in IoT.

Fink G. A., et. al	Security and privacy grand challenges for the internet of things [24]	2015	The paper highlights various kinds of vulnerabilities associated with the IoT that are expected to rise and presents a research agenda to marginalize the challenges.
Zhang Y.,	Technology Framework of the Internet of Things and Its Application [25]	2015	This paper presents a survey on IoT, all its organization and definition and its technology framework have been discussed in detail.

4. SECURITY FEATURES AT VARIOUS LAYER OF IOT

Each and every layer of IoT has to deal with many security concerns that needs to be addressed and tackled so that the security issues and threats to IoT framework is marginalized to great extent. Here we present few of the many security issues that exist in the existing layers of IoT architecture. The next section provides us with the review of few of the algorithms in concise manner that are implemented at various layers to solve the problem of security in IoT architecture.

Perception Layer deals with the sensing and reading of data by various sensors so there might be chances of some unauthorized sensor reading some confidential data. Along with reading of data the intruder or the attacker can even manipulate the data. The attacker can even try to block the RFID tag or barcode or any sensor resulting in loss of information. Since, the RFID tags are quiet visible to everyone there are chances that even the tags can be cloned which is highly undesirable. **Network Layer** deals with transfer of data through wireless communication network. The communication network can be based on various platforms like Bluetooth, cloud or Wi-Fi. The concerns of using these technologies are, for example in Bluetooth up to 7-8 devices can be paired simultaneously or even in Wi-Fi. If our IoT architecture is using one of such technologies without any security measures adopted at network layers for these technologies, the attacker can easily latch himself in one of the existing network and can easily steal or manipulate data leading to undesirable results. The service of IoT at **middleware layer** can easily be tampered by the attacker through unauthorized access. As the middleware layer provides us with data storage facilities so through unauthorized access the attacker can easily damage the system by removing the important data or changing it for his personal benefits, thus producing different unenviable results. Denial of service can be one such case in these types of attacks. **Application Layer** deals with the user end, so many illegal ways and hacking techniques can be adopted by the attacker to get hold of user data to damage or manipulate it, for example feeding with malicious program that can shut down the complete system or making the user access some malevolent software to gain access of the user data and tamper it such that the device starts to malfunction or even deny to provide its services. The algorithms can be implemented to tackle IoT security concerns at various layers are shown in Table 2 as given below.

Table 2: Various algorithms for security of IoT at various layers [26][27][28][29][30].

PERCEPTION LAYER	NETWORK LAYER	APPLICATION AND MIDDLEWARE LAYER
Hash algorithm	Point to point encryption	Intrusion detection techniques
RSA algorithm	Routing algorithm	Data mining
DSA algorithm		Anomaly detection.
Blowfish algorithm		Firewalls
DES algorithm		Spywares
K-anonymity algorithm		Malwares

4.1 RSA ALGORITHM

RSA algorithm was proposed by Rivest, Shamir & Adleman of MIT in 1977. It's one of the most widely known public key schemes. It is asymmetric kind of cryptography as it involves the use of both public and private keys. Different keys are used to encrypt and decrypt data. This type of algorithm ensures both confidentiality and authentication, which is the greatest advantage of this algorithm. The algorithm for confidentiality is shown in fig. 2 given below.

Steps for generation of public and private keys:

1. Generation of two prime numbers i.e. p and q
2. Calculation of modulus n = p*q
3. Selection of an integer e (should not be a factor of n)
4. Calculation of totient [ψ(n)] = (p-1)(q-1)
5. Calculation of mod d= [ψ(n)] ÷ e
6. Private key= [d,n]
7. Public key= [e,n]

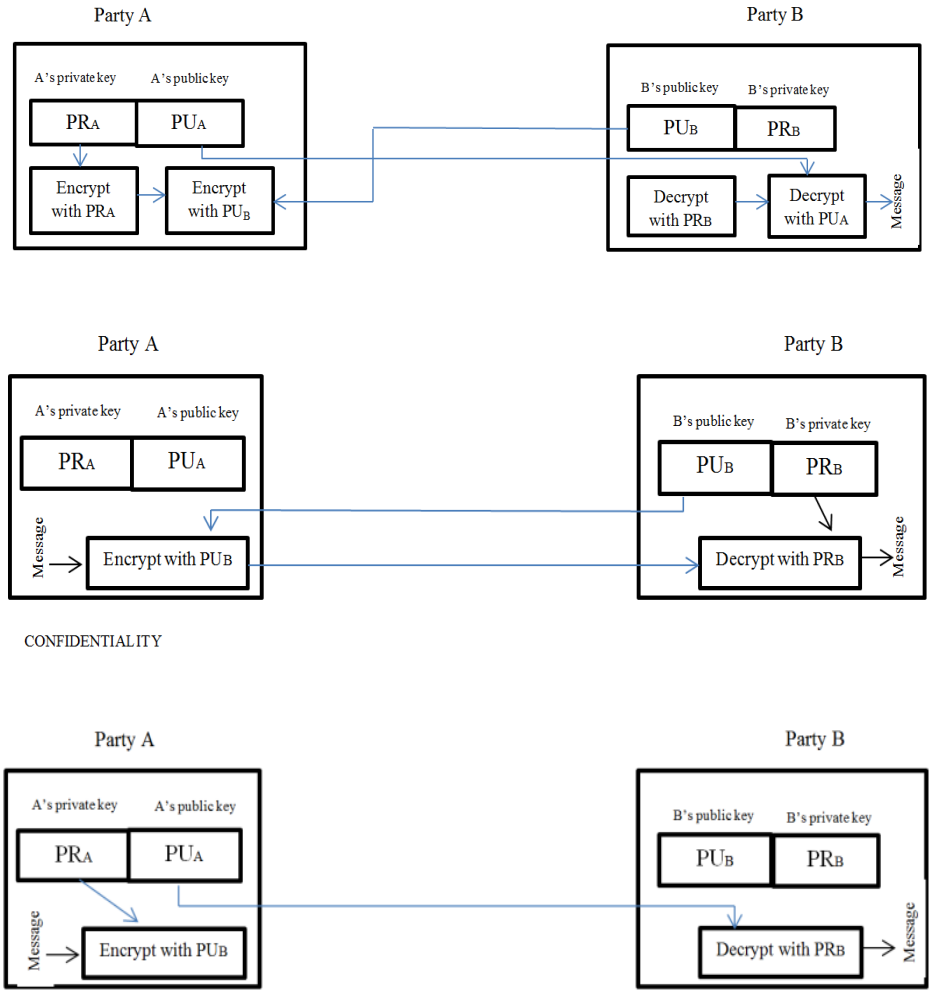

Figure 2: RSA encryption public-key cryptography method for confidentiality of data [29].

Demerits- As the computational efficiency of of factorization is improving day by day, RSA requires to deploy the use of larger keys. Keys of length 1024 bits are expected to be cracked down in the near future. Therefore, the key length of 2048 and 4096 bits are recommended.

4.2 BLOWFISH ARRAY

It is a symmetric type of encryption technique i.e. it uses the same key for both encryption and decryption. It was devised by Bruce Scheier in 1994. This is an open source, freely available and non-patented algorithm available for modifications. It has 2 arrays- p array has 18 blocks each containing 32 bits of data and 4 s arrays each containing 256 32- bit values. Plain text is divided into 64- bit block size. The algorithm is explained in fig. 3 as shown below.

Blowfish process has 16 rounds. Each round performs two tasks- key expansion and encryption.

Each round performs XOR and a function. Plaintext (32-bits) is XORed with P1 (32-bits).

For i=1:16
{
XL=XL XOR P1
XR=F(XL) XOR XR
Swap XL and XR
}
XL=XL XOR P17
XR=XR XOR P18
Combine XL and XR

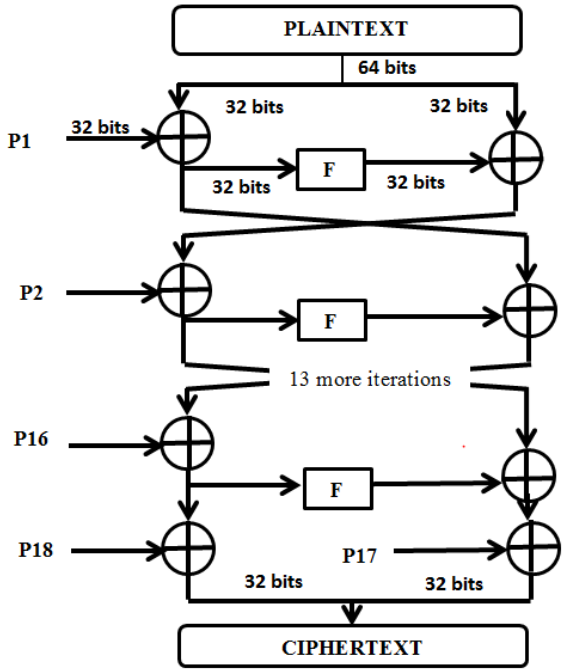

Figure 3: Block diagram of Blow Fish Algorithm [31].

Both RSA and Blowfish algorithms deal with the perception layer of IoT architecture. Out of these two algorithms RSA algorithm is a much secure option because it uses simultaneously two different keys that is public and private keys for transferring data so the authorized user doesn't needs to share his private keys for transferring data thus maintaining its security standard which is not the case with blowfish as this algorithm has only one key for sharing of information.

4.3 ROUTING PROTOCOLS

Some of the most commonly used routing protocols are Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). This particular section discusses routing protocols suitable for IoT devices.

RIP- It is an example of distance vector routing. In this type of routing, every router maintains its own routing table in which it contains information about all the nodes within the network. Information like destination address, estimated cost, hope count, time delay is incorporated in the vector routing table. Periodic update of each node's table is done either manually or automatically. One node periodically shares its table with every other node and each node compares its existing table with the shared table and looks for any updates.

OSPF- It is the most popular routing method. It uses link state routing technique. Each packet of data traverses through the shortest path calculated by the nodes. Each node maintains its own table. Dijikstra algorithm is used to calculate the shortest path. Initially, source is considered as the root node which analyses its each neighboring node for the shortest path to the destination.

BGP- It is an inter-domain routing protocol based on path vector routing system. It is used to connect between two or more autonomous system. It works in the same way as the distance vector routing protocol except for that there is a speaker node in each autonomous system that speaks i.e. shares its routing table with the speaker nodes of the neighboring autonomous systems. It is the most effective method among all the three stated as RIP and OSPF protocols are intra- domain routing protocols and BGP is an inter- domain networking.

The problem with Dijikstra algorithm is that it always searches for the shortest path routing. This can be beneficial for short term application but on long term basis, if there is a lot of traffic or there is a data overloading at a particular path then this algorithm fails as it cannot search for alternate path for transferring data.

4.4 INTRUSION DETECTION SYSTEM

Intrusion detection system is a method to detect unauthorized intrusion in to a system or network by any malicious intruder. Intruders may be from outside or inside the network. This detection technique is used to prevent the breakthrough of any suspicious person or activity within a network. The incoming packets of the network are sniffed for any aberrant pattern. When any violation is detected, alarm is raised and administrator is cautioned.

Three broad categories of intrusion detection algorithms are as follows-

1. Signature detection- It is based on the pre-defined signatures that is already known

to the system. Any deviation from the standard signatures raises an alarm of attack by an outsider. In other words, according to this technique, decisions are made on the basis of the comparison between the observed trend and the unusual trend. It has the biggest advantage that the attacks can be detected with a high probability with low false positive rate [7]. It is easier to implement and is lighter for the processing unit to handle. It has the drawback that it requires periodic update of signatures so that its database is up-to-date with all the signatures.

2. Anomaly detection- it creates a baseline for the network and all the activities in a system. Any deviation from the baseline is considered as an intrusion. If any intruder who does not have the idea of authentic user's pattern tries to break in a network then there is a maximum chance that such an activity will not undergo unnoticed. It has the advantage that it can easily detect new threats and also has the capability of detecting internal threats. However, the rate of rising fall alarms is more in this type as compared to the signature detection technique. Also, it has a constraint that every user profile should undergo a training period to create an appropriate profile to be considered as a standard. Maintenance of them is a cumbersome process.
3. Hybrid intrusion technique- it is the combination of both the techniques stated above. This type of method incorporates the merits of both the methods [32].

5. CONCLUSION

We all know that Internet of things is a technology that plays an integral part in technical advancement of our modern world. To reduce the complexity of IoT framework, IoT has been subdivided into different layers that work together to provide us with a giant interconnected network where each and every device are connected to each other in some way or the other. This provides us with a greater understanding of how IoT works and what all are its terminologies, but along with all these benefits, security is one of the major aspect of IoT which can't be overlooked or ignored. This paper provides us with various security issues that are present in every layer and can prove detrimental to IoT framework. Also, the paper highlighted some of the security measures and standard that can be implemented at various levels and how they work to enhance securities of various layers. Thus, we can conclude that IoT is serving our purpose in developing a smart environment for the growth of our civilization as we are leaping into next gen era, but the security discrepancies present in IoT layers should also be given a great importance as well to make utmost use of this technology for our development.

REFERENCES

[1] Jazib Frahim et. al, "Securing the Internet of Things: A Proposed Framework", available at http://www.cisco.com/c/en/us/about/security-center/secure-IoT-proposed-framework.html#2

[2] Deccan Chronicle, 2017, "Hajime IoT worm infects 300,000 devices" available at http://www.deccanchronicle.com/technology/in-other-news/280417/hajime-IoT-worm-infects-300000-devices.html

[3] Coppock M., 2017, "New 'BrickerBot' malware attack kills unsecured Internet of Things devices," available at https://www.digitaltrends.com /computing/brickerbot-malware-targets-IoT-with-pdos-attacks/

[4] Kulkarni R., 2017, "8 Malicious DDoS Attacks That Shook IoT," available at http://www.readitquik.com/articles/IoT/8-malicious-ddos-attacks-that-shook-IoT/

[5] Johnson J., 2017, "Internet of Insecure Things," https://www.scmagazine.com /internet-of-insecure-things/article/647880/

[6] Molnar D., and Wagner D., 2004, "Privacy and Security in Library RFID: Issues, Practices and Architectures," Proc. 11th ACM conference on Computer and communications security, Washington DC, USA, pp. 210-219.

[7] Mitrokotsa A., Rieback M. R., and Tanenbaum A. S., 2010, "Classifying RFID attacks and defenses," Information Systems Frontiers, 12(5), pp 491–505.

[8] Hancke, G. P., Markantonakis, K., and Mayes, 2010, "Security challenges for user-oriented RFID applications within the 'Internet of Things'," J. of Internet Technology, 11(3), pp. 307-313.

[9] Rolf H. W., 2010, Internet of Things - New security and privacy challenges," computer law & security review, 25, pp. 522–527

[10] Roman R. , Najera P., and Lopez J., 2011, "Securing the Internet of Things," IEEE Computer, 44(9), pp. 51-58.

[11] Khoo B., 2011, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," IEEE Proc. Internet of Things (iThings/CPSCom), 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, pp. 709-712.

[12] Liu C., Yang J., and Zhang Y.,2011 , "Research on Immunity-based Intrusion Detection Technology for the Internet of Things," IEEE Proc. Seventh International Conference on Natural Computation, Shanghai, China , pp. 212-216 .

[13] Clarke J., Castro R., Sharma A., Lopez J., and Suri N., 2012, "Trust & security

RTD in the internet of things: Opportunities for international cooperation," ACM Proc. First International Conference on Security of Internet of Things, Malaga, Spain ,pp. 172-178.

[14] Bhattasali T., Chaki R., and Sanyal S., 2012, "Sleep Deprivation Attack Detection in Wireless Sensor Network," Int. J. of Computer Applications, 40(15), pp.19-25.

[15] Suo H., Wan J., Zou C., and Liu J., 2012, "Security in the Internet of Things: A Review," IEEE Proc. International conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, pp. 648-651.

[16] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.

[17] Qiang C., Quan G. R., Yu B.,and Yang L., 2013 "Research on Security Issues of the Internet of Things," Int. J. of Future Generation Communication and Networking, 6(6), pp.1-10.

[18] Liu C., Zhang Y., and Zhang H., 2013, "A novel approach to IoT security based on immunology," IEEE Proc. International Conference on Computational intelligence and security (CIS), Leshan, China, pp. 771-775.

[19] Zhao K., and Ge L., 2013, "A survey on the internet of things security, " IEEE Proc. 9th Int. Conf. on Computational Intelligence and Security (CIS), Leshan, China, pp. 663-667,

[20] Roman R., Zhou J., and Lopez J., 2013, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, 57(10), pp. 2266-2279.

[21] Farooq M., Waseem M., Khairi A., and Mazhar S., 2015, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, 111(7).

[22] Mahmoud R., Yousuf T., Aloul F., Zualkernan I., 2015, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures," IEEE Proc. 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, pp. 336-341.

[23] Granjal, J., Monteiro, E. and Silva, J.S., 2015, "Security for the internet of things: a survey of existing protocols and open research issues," IEEE Communications Surveys & Tutorials, 17(3), pp.1294-1312.

[24] Fink, G.A., Zarzhitsky, D.V., Carroll, T.E. and Farquhar, E.D., 2015, "June. Security and privacy grand challenges for the Internet of Things," IEEE Proc.

International Conference on Collaboration Technologies and Systems (CTS), Atlanta, GA, USA ,pp. 27-34.

[25] Zhang, Y., 2011, "Technology Framework of the Internet of Things and its Application," IEEE Proc. International Conference on Electrical and Control Engineering (ICECE), Yichang, China, pp. 4109-4112.

[26] Salomaa, A., 2013, "Public-key cryptography," Springer Science & Business Media.

[27] Schneier B., 2005, "Description of a new variable-length key, 64-bit block cipher (Blowfish) Description of a New Variable-Length K," Springer Lecture Notes in Computer Science book series, Berlin, Heidelberg, vol 809.

[28] Tewari A., and Kumar A., 2014, "Different routing algorithm for computer networks," Int. J. of science, engineering & technology, 1(1), A3.

[29] Forouzon B. A., 2007, "Data communication and networking", 4th edition, McGraw-Hill Higher Education.

[30] Patcha, A. and Park, J.M., 2007, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer networks, 51(12), pp.3448-3470.

[31] Schneier B., 1994, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," In: Anderson R. (eds) Fast Software Encryption (FSE), 1993, Lecture Notes in Computer Science, vol. 809, Springer, Berlin, Heidelberg.

[32] Patcha, A. and Park, J.M., 2007, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer networks, 51(12), pp.3448-3470.