PBSE: A Lightweight Position Based Encryption/ Decryption Algorithm for IoT

Aswathy K (M. Tech Scholar), Suresh Kumar N (Associate Professor)
Dept. of Computer Science & Engineering
College of Engineering and Management, Punnapra
Kerala, India
Email: aswathykmtech@gmail.com, cnsuresh2000@gmail.com

Abstract**—**Internet of Things(IoT) is an emerging technology now a day which makes the life of human beings smart through the use of different objects, but it faces many issues concerned with security. Different types of attacks can happen in various layers of IoT architecture. This work discusses about various attacks, security mechanisms and their methods that used to resolve such issues. It also proposes a new and simplified lightweight position based encryption/decryption method that can be used to secure the data of users. The proposed algorithm is less computational intensive that offers less encryption and decryption time with respect to standard encryption algorithms like AES and is simple to use.

Keywords**—***IoT security; attacks; mechanisms; PBSE algorithm*

I. Introduction

Modern world is the world of Internet. Now-a-days, we are living in a “smart world” consisting of different smart objects including home appliances, vehicles, electronic equipments etc. The technology involving communication and actuation among these equipments is referred as "Internet of Things" which consists of many layers. The layers of IoT architecture are mainly classified as Perception layer, Network layer, Middleware layer and Application layer, and are illustrated in Fig. 1[2]. Perception layer focuses on collection of data using sensors, RFID tags etc. Network layer makes the communication possible through various parts in the network such as Internet, satellites and communication protocols. Application layer make use of computers, mobile phones etc., to access to the Internet through interfaces and this layer is responsible for providing services to users as per user’s requirements[1]. Middle ware layer is actually a service oriented layer that makes use of cloud computing and other storage measures for providing storage capabilities [2]. Internet of Things is applicable in various fields such as home automation, environment monitoring, smart city, smart grid, and healthcare applications etc., depicted in Fig. 2 [18].

Various security attacks can happen in different layers of IoT. Some of the attacks are Denial of Service (DoS) attack[21][22], phishing[23][24][25][26], spoofing[27][28], Sybil attack[29][30], tag cloning[31][32][2] etc. Different security mechanisms can be implemented to mitigate such attacks. It include authentication and access control [11], trust management [12], encryption [13] [17], secure routing [14] and intrusion detection [15]. These mechanisms are analyzed in detail in the following sections.

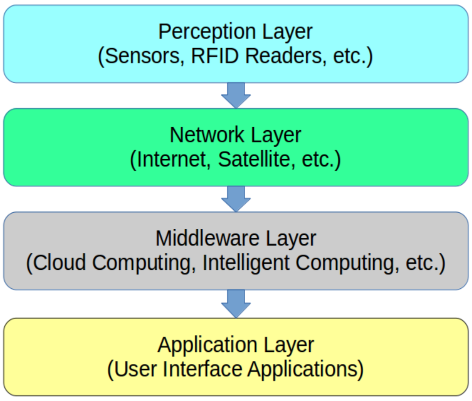
Perception Layer
(Sensors, RFID Readers, etc.)
Network Layer
(Internet, Satellite, etc.)
Middleware Layer
(Cloud Computing, Intelligent Computing, etc.)
Application Layer
(User Interface Applications)

Figure 1: The layers of IoT architecture

This paper is organized as follows. Section II shows the related work, section III portrays the security threats in IoT scenario, section IV describes various countermeasures for IoT attacks, section V proposes a new position based encryption algorithm, section VI describes the performance evaluation of the proposed algorithm with respect to tiny AES[20] algorithm and the section VII is the Conclusion and future directions.

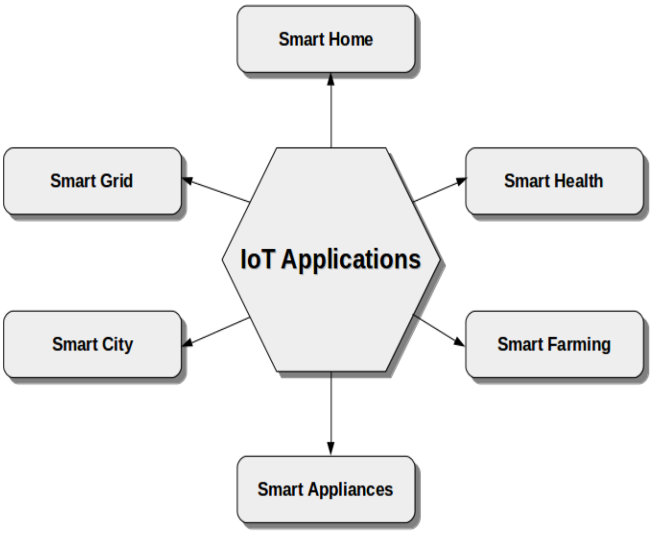

Figure 2: Applications of IoT

II. Related Works

Various security attacks in IoT scenario are classified in [3], which consist of physical attacks, network attacks, software attacks and encryption attack. Physical attacks include node tampering, RF interference, malicious code injection and physical damages. Network attacks are causing interruption in communication network, including traffic conjunction [33], DoS attack, spoofing, cloning etc. Software attacks are caused by the malicious codes such as virus, worms, spyware and Trojan horse. Encryption attacks include all attacks harming the plain text and cipher text and man-in-the-middle attack in which an intruder communicate with two legitimate users, in middle of them, but each of the legitimate parties believe that they are communicating with the authorized one.

The attacks happening in RFID are classified in [4]. RFID attacks can occur in any of the layers of IoT architecture. Countermeasures that can be used to avoid such attacks include disabling of RFID tags, eavesdropping, relay attack, tag destruction etc.

The author of [5] reviewed the possible Jamming attacks that occur in an IoT network. Jamming can be considered as a special type of DoS attack. This work describes different types of jamming such as spot jamming, sweep jamming, barrage jamming and deceptive jamming. It also explains some security schemes against jamming in WSNs.

Trust evaluation is considered as a serious security issue in [6], [7], [8] and [9]. These works describes about trust management protocols and trust evaluation properties such as honesty, cooperativeness and community-interest. Different metrics such as End-to-end Packet Forwarding Ratio (EPFR), Energy Consumption and Packet Delivery Ratio (PDR) are presented [6].

Different security mechanisms can be implemented to overcome these security issues. Some of the main concepts are explained in [10], which reviews security mechanisms on different layers of IoT, current security issues, their corresponding mechanisms and popular tools used for implementing them.

III. Security Threats in IoT Scenario

IoT security issues can be classified on the basis of different layers of IoT. Various attacks can happen in Perception layer, Network layer, Middleware layer and Application layer, and these are classified in Table 1[2][10].

TABLE 1: Attacks on different layers of IoT

Layers	Possible Attacks
Perception Layer	Tag cloning[31][32], Spoofing[27][28], Jamming[5][34], Eavesdropping[4]
Network Layer	DoS attack[21][22], Man-in-the-middle attack[35], Sybil attacks[29][30], Sinkhole attacks[36][37]
Middleware Layer	DoS attack, Malicious insider[38], Unauthorized access[39]
Application Layer	Phishing[23][24][25][26], DoS attack, Malicious codes[40]

(1) Tag Cloning

Tag cloning is one of the serious attacks that can cause even financial loss to some commercial applications. The attackers need to know only the RFID tag ID to clone it. Cloning refers to the copying of RFID tag ID, which results in two RFID tag with same identification number [4][31][32].

(2) Spoofing

In this attack, the attacker tracks RFID signals to read and record data transmissions from RFID tags of the victim. The attacker can send his own data containing the original RFID tag ID, making it appear to be valid. In this way, the attacker gains full access to the system pretending to be the original one [3][4][27][28].

(3) Jamming attacks

Jamming is a type of attack that directs an electromagnetic energy towards a system to disrupt the communication signals or to make inconvenience. Interference of radio frequencies are one of the main source of jamming attack. This type of attack can be viewed as a special case of DoS attack [5][34].

(4) Eavesdropping

Eavesdropping is a type of attack in which an attacker uses antenna to trace information of an authorized user. This information is recorded and can be used for performing more attacks or any illegal activities. This occurs between RFID tag and reader. It depends on the distance between the RFID device and the attacker [4].

(5) DoS attacker

DoS attack is a serious attack in which the intended users of a service becomes inaccessible to it because of the flooding of target site or sending information that makes the system crash. In this, an attacker send thousands of messages to a particular site, that the system cannot handle, which results in the crash of the site[21][22].

(6) Man-in-the-middle attacker

In this attack, the attacker comes between the communications of two authorized parties, but they are unaware of the middle attacker. They communicate to each other, but in real, they are communicating with the intruder. The intruder can see and modify the information they are sending to each other [35].

(7) Sybil Attacks

In this attack, a challenger node or competitor node supposes identity of multiple nodes, which results in the inefficiency in the network. In such circumstances, there are some chances of starvation in some nodes of network. This occurs in a network with non-verified nodes [29] [30].

(8) Sinkhole attacks

Sinkhole attack is a type of attack in which the intruder tries to attract the neighboring nodes by providing false routing updates. The intruder tries to create a sphere of influence which results in the launching of many other attacks [36] [37].

(9) Phishing

Phishing is an application layer attack in which the attacker tries to steal confidential information of a user such as user names, passwords etc. In this, the intruder masquerades as a trusted entity and sends emails or other messages to the victims. The information entered by the victim are compiled and stored by the attacker for accessing the network [23] [24] [25] [26].

(10) Malicious codes

Malicious codes are pieces of codes in a software that are intended to make harm effects including security breaches or complete destruction of the system. There are various categories of malicious codes such as virus, worms, logic bombs, Trojan horse etc [40].

IV. Countermeasures for IoT Attacks

There are several security mechanisms to mitigate the security vulnerabilities in an IoT system. Some important security mechanisms are described in the following section.

(a) Authentication

Authentication [11] is the process of proving that the entities which are participating are genuine. There are different kinds of authentication methods. Each of them are explained below.

(i) ID/password pairs

This is the common way of authentication, in which each authenticated must provided with a user name and password. By using these, one can enter into the system. If they are entered wrong by an entity, he cannot enter to that system. Most of the online systems are using this type of authentication technique. The passwords entered by the user are stored in special files in an encrypted form. The main advantages of this system are it is simple and easy to use. The disadvantage is it can be easily forged or stolen by a third party [11].

(ii) Biometrics authentication

In this, different parts of a human body are used for identification purpose. Mainly using body measurements are finger prints, eye, face of a person etc. The possibility of forging and stealing is comparatively less in this. But, sometimes it states legitimate users as wrong and illegitimate users as true users. It cannot be considered as completely true [11].

(iii) Dynamic authentication

Dynamic authentication schemes are using one time password systems, which is considered as a complete solution to unauthentication problem. Different dynamic authentication schemes used are code book, time based and challenge-response based [11]. All of these techniques are generating one time passwords that are valid up to a time period. This is the most secure authentication scheme [11].

(b) Trust Management

Trust is an important factor to be considered in a secure system. The behavior analysis of each component of the system is done in trust evaluation schemes. If the components are producing untrustworthy behavior, the system cannot be considered as a secure one. Different types of trust that are to be evaluated are data perception trust, identity trust, transmission and communication trust, user trust and IoT application trust [12].

(i) Data Perception trust

The trust in Perception layer of IoT architecture is concerned in this scheme. Perception layer includes sensors and RFID tags. The integrity and analysis of data obtained from these devices are evaluated here. It concerns about different privacy issues related to RFID technologies and physical security of the devices [12].

(ii) Identity trust

Privacy preservation is an important objective of trust management. Identity of each entity should be legitimate in a secure system. The entry of an illegitimate user can entirely destroy the system. So, identity trust need more focus in a secure system. Some works mainly focuses on virtual identities as a representation of all kinds of entities [12].

(iii) Transmission and Communication trust

A good IoT system must support heterogeneous devices which becomes the challenge of the IoT system. The trust evaluation should done in network layer of the system. The transmission and communication of data should be done between authorized users. For enhancing security, lightweight symmetric encryption and different asymmetric encryption schemes can be used. Different intrusion detection mechanisms and routing protocols can be implemented for a trustworthy network operation [12].

(iv)User trust and IoT application trust

The users of IoT system must be trusted on the operations of the system. There are a large variety of IoT applications used in day to day life. Trust evaluation is an important criteria in their implementation. Not all applications are implementing all the objectives of trust management. Trust management and evaluation is an emerging area of IoT research [12].

(c) Encryption

Encryption and decryption are two important parts of any secure system. In the field of cryptography, many symmetric and asymmetric algorithms are used. But, it is not completely verified that whether all these algorithms can be used IoT systems. Mainly, some lightweight encryption methods are used in IoT. Symmetric algorithms such as Advanced Encryption Standard (AES) and High security and lightweight (HIGHT) are mainly used for encryption. The main objective of AES is preserving confidentiality [13].

Some asymmetric algorithms can also be used, but they are not lightweight because of their large key size. The main asymmetric algorithms are RSA and ECC (Elliptic Curve Cryptography). Both of these algorithms can be used to preserve digital signature. A new algorithm HLA (Hybrid Lightweight Algorithm) which is a combination of both lightweight symmetric and asymmetric algorithms is proposed in [13]. It provides confidentiality and integrity with small key size.

(d) Secure Routing

Providing security is one of the main objectives of an IoT network. Routing should be secure in an IoT system because IoT system consists of different heterogeneous devices and networks. These objectives are implemented using different routing protocols. Some of the protocols are secure multi-hop routing, a Trust aware secure routing framework (TSRF), Two-way acknowledgement trust (2-ACKT), Group-based trust management scheme (GTMS) and Lithe (Lightweight secure CoAP). Comparison of these protocols is illustrated in Table 2. The main features considered are the complexity and scalability of each protocol [14].

(e) Intrusion detection

Intrusion detection is referred as the process of finding intruders that cause malicious activity in a network. Intrusion detection system (IDS) is a piece of software that helps to find the intruders. There are several intrusion detection methods namely signature-based, anomaly-based, specification-based and hybrid approaches. Each of these methods are described in detail [15].

(i) Signature-based intrusion detection

In this approach, when an attack occurs in the system, the IDS detect the attack if it is stored in the IDS internal database. Each known attacks are stored in the IDS internal database with their specific signature. Using this approach, it is helpful in detecting known attacks. But, if an unknown attack came to the system, this method becomes ineffective [15].

(ii) Anomaly-based intrusion detection

This approach is helpful in detecting new attacks, especially attacks related to resources. This approach regularly checks the activities of a system at a time, and compare whether it is deviating from the normal behavior of the system. If the behavior exceeds a threshold limit, the activity is considered as an attack [15].

TABLE 2: Comparison of various secure routing protocols

Protocols	**Complexity**	**Scalability**
Secure Multi-hop protocol	Low	Medium
TSRF	High	No
2-ACKT	Medium	Not Available
GTMS	High	High
Lithe	High	No

(iii) Specification-based intrusion detection

This intrusion detection works on the basis of some specifications given to the system about the attacks. Specifications can be considered as a set of rules that define the normal behavior of the system. It is similar to an anomaly-based approach; the difference is that the rules or the specifications can be given manually to the system [15].

(iv) Hybrid approach

Hybrid approaches are the combination of signature-based, anomaly-based and specification-based intrusion detection methods. The main reason for developing this approach is that it can maximize the advantages and minimize the drawbacks of each method. Each kind of approach may fail in any of the attacks to detect. A combination of these three may create a better intrusion detection environment in an IoT system [15].

(f) Access Control

Access control [11] in an IoT system allows only authorized users to access or use the system or resources such as sensors and other devices. Access control mechanisms can be classified mainly into three, namely Role-based access control (RBAC), Attribute-based access control (ABAC)[19] and Usage control.

(i) RBAC

The illustration of access control problems are done through access control matrix, in which users are represented in rows and the available resources are represented in columns. The role-based access control is a type of access control mechanism which describes the access control matrix in an abstract way. In this, each user has a specific role and there are some permission given to them. Based on these permissions, they are associated with the resource [16][19].

(ii) ABAC

This technique is more abstract than RBAC technique. In this, each user is associated with an access policy. The access policy describes some user attributes such as name, job etc., and each resource have attributes which describe some conditions that must be satisfied before access is granted [19].

(iii) Usage Control

RBAC and ABAC can be classified as classical access control mechanisms. Beyond these, the new model introduced is the Usage Control (UCON) model. In this, it enables control over usage of digital objects than that of traditional access control policies and models [16].

From the above papers, the following conclusions are derived:

- IoT devices are lightweight devices, hence the standard encryption algorithms available in the literature cannot be directly used
- There is a need to develop lightweight encryption algorithm that offers low encryption time but provide moderate security. Different algorithms are developing by the technical experts that provide both security and lightweight also.
- Among various security mechanisms that can be used in IoT environment, the most popular mechanism is the authentication method. Trust management is in the development stage. Encryption mechanism provides more security, but it is rarely used because of difficulties in the process of key generation and the need of encryption and decryption at suitable phases [10].
- Taking these factors into consideration, a position based encryption/decryption algorithm that offers low encryption time and moderate security and easy to run at lightweight devices is proposed.

V. Position Based Simple Encryption (PBSE) Algorithm

This section proposes a new position based encryption algorithm which is not based on the characters, but on the position of characters. The algorithm is described below.

Algorithm

Input: Plain text as plain_text [100]

Output: Cipher text as cipher_text [100]

Encryption Function

```
1. Start
2. Find the length of the plain_text and let it be len
3. For each i from 0 to len-1, do the following steps
    3.1 Set c = plain_text[i]-32 //to avoid non-printable ASCII characters which are till 31
    3.2 Set x = i mod 26 // to avoid excess increase in position variable while doing position based encryption. 26 is an arbitrary value to limit the position variable.
    3.3 Set key = $2x^2 + 3x + 7$ // a quadratic equation of the form $ax^2+bx+c$ to find the key for position based encryption
    3.4 Cipher_text[i] = (c+key) mod95 + 32 // Adding the key to convert the plain text to printable encrypted form within the ASCII limit, i.e., 32 to 126.
4. Stop
```

Decryption Function

```
1. Start
2. Find the length of the cipher_text and let it be len
3. For each i from 0 to len-1, do the following steps
    3.1 Set c = cipher_text[i]-32 //to avoid non-printable ASCII characters which are till 31
    3.2Set x = i mod 26 // to avoid excess increase in position variable while doing position based encryption. 26 is an arbitrary value to limit the position variable.
    3.3Set key = $2x^2 + 3x + 7$ // a quadratic equation of the form $ax^2+bx+c$ to find the key for position based encryption.
    3.4 Reverse of step 3.4 of encryption. Subtract the key.
4. Stop
```

The plain text and cipher text are represented using arrays. The length of plain text is calculated. Since there are 33 non printable characters (0 to 31 and 127) at the beginning of the ASCII character set, subtraction by 32 is done for each character in plain text. In this algorithm, 'i' is the actual position variable. The key is generated with the position variable in a quadratic equation. As the size of position variable increases, there are chances of overflow of the key variable. So, for the purpose of limiting the position variable, another variable x=i mod 26 is used in the quadratic equation. The value 26 and the quadratic equation $2x^2 + 3x + 7$ are arbitrarily selected. The user can use any quadratic equation of the form ax^2+bx+c as a key generator, provided the same quadratic equation must be used in the decryption side also. As there are 95 printable characters in ASCII character set, while calculating cipher text, the key is added with the plain text character and mod 95 is done with that value. After that, 32 is added to make it a printable character. The same steps are repeated in the decryption function, except that subtraction by key value is done in decryption while addition with the key value is done in encryption.

VI. Performance Evaluation

The simulation of tiny AES algorithm and PBSE algorithm is done in Contiki Cooja platform. The experiment is done with sky mote and performance is calculated in three types of data-small data consists of only 10 characters, a medium size data of 36 characters and a large data of 61 characters. The encryption time and decryption time is calculated for these data in Cooja and graph is generated for the same. From this example, it is found that the encryption time is slightly greater than the decryption time in the case of PBSE, meanwhile the decryption time of tiny AES algorithm is large when comparing with the encryption time of the same.

AES is a well known encryption algorithm that provides a very good security comparing with other algorithms. Tiny AES is a variation of AES algorithm which is compatible only with small size of data. AES generally supports 128 bits of data and tiny AES supports 64 bits of data. But in IoT scenario, some other features like encryption time, decryption time etc., are considered more rather than security.

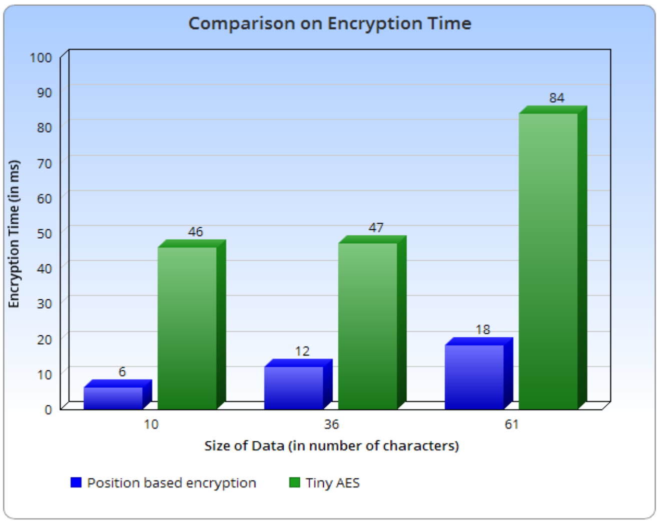

Figure 3: Comparison on Encryption time

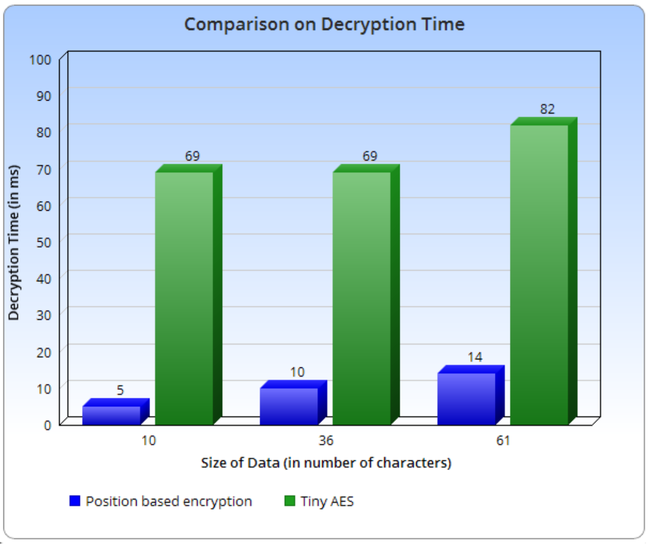

Figure 4: Comparison on Decryption time

Comparing the proposed PBSE algorithm with tiny AES algorithm, it is found that the encryption time and decryption time of PBSE is very low than the tiny AES algorithm, but only with a moderate security. Although security is more in AES algorithm, it is not directly adaptable to IoT lightweight devices. Fig. 3 and Fig. 4 illustrate the comparison of encryption time and decryption time, respectively, of both PBSE algorithm and tiny AES algorithm. PBSE algorithm is simple and easy to implement in IoT scenario.

VII. Conclusion and Future Works

This work describes about various security issues in different layers of IoT architecture. It also provides different mechanisms that can be implemented to mitigate the security risks in an IoT system. A new position based encryption algorithm is proposed in this work. The performance evaluation in terms of encryption/decryption time of text with variable size compared with respect to standard AES. The result shows that the proposed method offers better encryption/decryption time with respect to standard encryption algorithm. Implementation of an open source framework that utilizes various security and privacy mechanisms for IoT in a single window is considered as a future work.

References

[1] Jiafu Wan, Caifeng Zou, and Jianqi Liu, “Security in the Internet of Things: A Review”, International Conference on Computer Science and Electronics Engineering, 2012.

[2] M.U. Farooq, Muhammad Waseem, Anjum Khairi and Sadia Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015.

[3] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi, “Internet of Things: Security Vulnerabilities and Challenges”, IEEE, 2015.

[4] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, “Classification of RFID Attacks”, citeseer, 2010

[5] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, “A Survey on Jamming Attacks and Countermeasures in WSNs”, IEEE Communications Surveys & Tutorials, VOL. 11, NO. 4, Fourth Quarter 2009.

[6] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang, “TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things,” Computer Science Information System, 2011.

[7] Dennis Gessner, Alexis Olivereau, Alexander Salinas Segura and Alexandru Serbanati, “Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[8] Fenye Bao and Ing-Ray Chen, “Trust Management for the Internet of Things and Its Application to Service Composition”, IEEE international symposium, 2012.

[9] Yosra Ben Saied, Alexis Olivereau, Djamal Zeghlache and Maryline Laurent, “Trust management system design for the Internet of Things: A context-aware and multi-service approach”, Computer and security, Elsevier, 2013

[10] Mardiana binti Mohamad Noor and Wan Haslina Hassan,”Current research on Internet of Things (IoT) security: A survey”, Elsevier, Computer Networks, 2018.

[11] Jing Liu and Yang Xiao and C.L. Philip Chen, “Internet of things’ authentication and access control”, Int. J. Security and Networks, Vol. 7, No. 4, 2012.

[12] Zheng Yan, Peng Zhang and Athanasios V. Vasilakos, “A survey on trust management for Internet of Things”, Journal of Network and Computer Applications, Elsevier, 2014.

[13] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon and Jong Hyuk Park, “Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions”, J Ambient Intell Human Computer, Springer, 2017.

[14] David Airehrour, Jairo Gutierrez and Sayan Kumar Ray, “Secure routing for internet of things: A survey”, Journal of Network and Computer Applications, Elsevier, 2016.

[15] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani and Sean Carlisto de Alvarenga, “A survey of intrusion detection in Internet of Things”, Journal of Network and Computer Applications, Elsevier, 2017.

[16] Mohamed Abomhara and Geir M. Køien, “Security and Privacy in the Internet of Things: Current Status and Open Issues”, IEEE, 2014.

[17] Xinlei Wang, Jianqing Zhang, Eve M. Schooler and Mihaela Ion, “Performance Evaluation of Attribute-Based Encryption: Toward Data Privacy in the IoT”, Communication and Information Systems Security Symposium, IEEE ICC 2014.

[18] Sajjad Hussain Shah and Ilyas Yaqoob, “A Survey: Internet of Things (IOT) Technologies, Applications and Challenges”, 4th IEEE International Conference on Smart Energy Grid Engineering, 2016.

[19] https://www.intopalo.com/blog/2015-05-25-access-control-for-internet-of-things/

[20] https://github.com/kokke/tiny-AES-c/blob/master/aes.c

[21] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC, “Distributed Denial of Service Attacks”, IEEE, 2000.

[22] Amey Shevtekar, Karunakar Anantharam, and Nirwan Ansari, “Low Rate TCP Denial-of-Service Attack Detection at Edge Routers”, IEEE Communications Letters, April 2005.

[23] Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, “A Framework for Detection and Measurement of Phishing Attacks”, ACM Workshop, 2007.

[24] Engin Kirda and Christopher Kruegel, “Protecting Users Against Phishing Attacks with AntiPhish”, IEEE, 2005.

[25] Ram Basnet, Srinivas Mukkamala, and Andrew H. Sung, “Detection of Phishing Attacks: A Machine Learning Approach”, Springer, 2008.

[26] Pawan Prakash, Manish Kumar, Ramana Rao Kompella and Minaxi Gupta, “PhishNet: Predictive Blacklisting to Detect Phishing Attacks”, IEEE, 2010.

[27] Abdenour Hadid, Nicholas Evans, Sébastien Marcel and Julian Fierrez, “Biometrics systems under spoofing attack: an evaluation methodology and lessons learned”, IEEE, 2015.

[28] Zhizheng Wu, Eng Siong Chng and Haizhou Li, “Detecting Converted Speech and Natural Speech for anti-Spoofing Attack in Speaker Recognition”, Edinburgh Research Explorer, January 2012.

[29] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons and Abraham Flaxman, “SybilGuard: Defending Against Sybil Attacks via Social Networks”, ACM, 2006.

[30] Qinghua Zhang, Pan Wang, Douglas S. Reeves and Peng Ning, “Defending against Sybil Attacks in Sensor Networks”, IEEE, 2005.

[31] Mikko Lehtonen, Daniel Ostojic, Alexander Ilic and Florian Michahelles, “Securing RFID systems by detecting tag cloning”, Springer, 2009.

[32] Jemal Abawajy, “Enhancing RFID Tag Resistance against Cloning Attack”, IEEE, 2009.

[33] JP Vasseur, A Di Pietro and JC Mota, “Traffic Segregation in DDos attack Architecture”, Google Patents, 2016.

[34] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, ACM, 2005.

[35] F Callegati, W Cerroni and M Ramilli, “Man-in-the-Middle Attack to the HTTPS Protocol”, IEEE, 2009.

[36] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos and Marios Mpasoukos, “Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks”, Springer, July 2007.

[37] Soo Young Moon and Tae Ho Cho, “Intrusion Detection Scheme against Sinkhole Attacks in Directed Diffusion Based Sensor Networks”, International Journal of Computer Science and Network Security, July 2009.

[38] Mark Maybury, Penny Chase, Brant Cheikes and Dick Brackney, “Analysis and Detection of Malicious Insiders”, International Conference on Intelligence Analysis, 2005.

[39] MS Edelman, “System and Method For Preventing Unauthorized Access To Electronic Data”, Google Patents, 2005.

[40] RS Hoefelmeyer and TE Phillips, “System and Method for Malicious Code Detection”, Google Patents, 2006.

Aswathy K is M.Tech scholar in Department of Computer Science, College of Engineering and Management Punnapra affiliated to APJ Abdul Kalam Technological University. She has complted her bachelor degree from Ilahia College of Engineering and Technology in 2014. Her area of interest includes Internet of Things and Protocol verification. She can be reached at aswathykmtech@gmail.com.

Mr. Suresh Kumar N is working as Associate Professor in the Department of Computer Science and Engineering, College of Engineering and Management, Punnapra. His research interests include Protocol verification, IoT Protocols, Protocol Modeling, Machine learning and Cyber physical systems. He can be reached at cnsuresh2000@gmail.com.