ISSN : 2350-0743

www.ijramr.com

*International Journal of Recent Advances in Multidisciplinary Research*
*Vol. 04, Issue 11, pp.3038-3041, November, 2017*

# RESEARCH ARTICLE

## IoT SYSTEM SECURITY: CHALLENGES AND PROSPECTIVE SOLUTIONS

***Santhi, H., Gayathri, P. Geraldine Bessie Amali and Gopichand**

School of Computer Science and Engineering, VIT University, Vellore, India

**ARTICLE INFO**

***Article History:***
Received 09th August, 2017
Received in revised form
27th September, 2017
Accepted 04th October, 2017
Published online 30th November, 2017

***Keywords:***
Authentication, Confidentiality,
Internet of Things (IoT),
Privacy, Security, Integrity.

**ABSTRACT**

The increasing demand and use of IoT systems has no doubt made our lives very easy and comfortable. With day by day growth of technology, new kinds of attacks and threats are occurring each day. Therefore, it is necessary to ensure the security of our networks and data. This paper tries to look at a variety of security problems that can be faced in the IoT Systems and their prospective solutions given by various authors. In the end, a comparative study of the problems addressed and the solutions given in each of the paper is done.

## INTRODUCTION

Internet of Things, IoT, is the most growing technology in today's time. The increased use of smart phones, androids and vast availability of internet add to its growth rate. The scope of IoT begins right from the sensor devices used to percept data, the network used for transmission to the application servers. IoT has moved human activities towards full automation. The IoT System is divided into three layers, namely, perception layer, network layer and application layer. With the immense flow of important data in the IoT Network, security is becoming a major concern for such systems. The security aspects and measures are to be applied to each of the layers of the IoT system and even to the low level devices. The system is vulnerable to a huge number and kinds of threats which need to be dealt in different ways for different devices.This paper first highlights the related research work and solutions proposed in this field by 10 different research publications. The next section gives a comparative study of their work.

### Related Work

In (Premnath and Haas, 2015), the author has tried to highlight the benefits of using smaller cryptographic key sizes for the encryption and protection of tactical data. Tactical data requires security only for a few days like a month or 15 days rather than for a longer period such as a decade or more than that. The author has highlighted this fact by an example of a smart grid network where smart meters are used to measure the energy consumption and pass on this data to the utility companies. This data can be tracked by an external entity and can be used to make conclusions based on the energy consumptions by any customer for example analysing that an owner is not at home if the electricity consumption is very low for a day or two and this information can be used to carry out burglary at the owner's house. This information is needed to be encrypted only till the house owner returns back, therefore suggesting the need of encryption only for a few days. In (Premnath and Haas, 2015), the author has compared the computational efforts of 3248-bit asymmetric/public key modulus to 1024-bit modulus using the formula *Effortrel* (*n*) = ((n^3)/ (3248^3)). The formula shows that the computational effort is only 3.1% of the computational efforts for that of 3248 bit-modulus. Using smaller keys also reduces energy consumption by the IOT nodes. Also, the author in conjugation with Moore's law show how to estimate the cost of breaking small sized cryptographic keys in terms of number of days and associated cost. Further it can be said that if the technology grows at a rate higher than the Moore's law then a larger bit modulus value will be needed to secure the data and if the technology grows at a rate lower than that of Moore's law then a lower bit modulus rate is needed to secure the data. The author has concluded with the statement that if the size of the key is selected in accordance with the time and budget adversary then the processing load for the IOT nodes can be reduced drastically. This strategy of using small sized cryptographic keys can be used only for data which requires encryption/security only for a short span of time and the results can be reversed if the technology grows faster than the Moore's Law. In (Schurgot *et al.,* 2015), the author has focused on the privacy and security of IOT systems using an inexpensive home automation system using cryptographic measure and manipulation of user data to prevent it from hackers inside the IOT networks or those who have compromised the remote servers. For this analysis, the author aims to use Commercial off the shelf (COTS) products which

***Corresponding author:* Santhi, H.,**
School of Computer Science and Engineering, VIT University, Vellore, India.

use cloud based servers, smart phones and web based applications to set up a minimal home automation system. Privacy attacks can occur when home sensor data is sent to remote locations for analysis and allows unauthorised access to third party data centres. An adversary can use these sensed data in order to cause harm to the occupant. The architecture of the home automation system consists of IOT devices connected to centralised cloud servers to control sensing reporting. The devices are connected to the network using a hub. SmartThings hub and app is used for communication. To conceal the user's location, the auther has proposed to use a VPN server to proxy the communication between the user and the cloud services. It the experiment, the VPN servers were installed in various remote locations to see if it caused any failures. There were no failures but it does introduce delay in the delivery of message depending on the VPN server's location. A fake GPS location app was used to spoof the location of the owner's android device. Momentory loss in the connection of the VPN server may occur due to presence of inactive hub or switch. Three techniques were used to manipulate event reporting as it's patterns could be used to track daily activities of the user.

- **Delaying events:** Delaying the events caused delay of conditional actions and therefore confuses the third person.
- **Inserting events:** these deception techniques will prevent the third person to see that the house is empty.
- **Deleting Events:** This includes dropping the events until the buffer is filled. This will lead the observer to assume that the there are some connection problems in the house.

In (Tiburski *et al.,* 2015), the authors have highlighted the importance of a security architecture in SOA (service-oriented architecture) based IoT Middleware. They have analysed the current architecture and suggested other measure to ensure more security. An IoT Middleware provides device abstraction, data management and development of the device and its architecture is based on SOA based standards. The amount of flow of data in these middlewares demands a security standard to be set for reference, which currently does not exist.

According to (Tiburski *et al.,* 2015), the attacks can occur in three forms:

- **Entities attacks:** related to unauthorised access and physical attacks on the application, middleware or device.
- **Data attacks:** when data is changed or spied between its transmissions.
- **Communication channel attack:** when communication channel between systems is attacked.

The author has proposed few security requirements to ensure security of the SOA based middleware systems. These are Authentication, Authorization and Access Control, Communication channel protection, Data Confidentiality and Data Integrity.

In (Gou *er al.,* 2013), the author has highlighted the need for security of IoT Systems and proposed suitable measure for the same. According to them, the IoT systems have three layers: the perception layer, network layer and application layer. The perception layer is the lowest layer of the system and is a source of access to information throughout the IoT. Physical security of the sensing device and security of information collection are the main issues of this layer. The proposed solutions for these issues are:

- Dividing the perception layer into subsystem levels of security according to the requirements of the pplication, so that each level of security has security element and scope.
- Strengthening key management system.
- Establishing a secure routing.
- Strengthening the node authentication and access control mechanisms.
- Establishing an effective an intrusion and fault tolerance mechanisms.

The network layer security issues include illegal access, data eavesdropping, confidentiality, integrity, destruction, denial of service attack, man in the middle attack etc. To minimise these security threats, proper authentication mechanisms can be used. Filtering and detection mechanisms can be used for data security. End to end authentication and key negotiation mechanisms can be used to prevent attacks like denial of service. The security issues in the application layer can be avoided by access management, data security, security management and cryptographic algorithms to encrypt the database. Along with these strategies, a series of laws, policies and regulations should be made to improve safety of IoT Systems.

In (Liu *et al.,* 2013), a novel approach to IoT security is proposed on the basis of immunology. Due to the large amount of data and attributes of dispersity, a dynamic frame is proposed. The current tradition network security systems are based on access control, authentication, security protocol, encryption, protection and privacy and therefore form a passive defence strategy. Therefore, there is a need for active defence is there. The proposed model consists of a security frame consisting of 5 links: Security threat detection, danger computation, security response, security defence strategy formation and security defence. The output of each of these links forms the input for the other link. Detectors are used to recognise the antigens and activate the memory detector. The danger computation link calculates the harm that can be caused based on the harmfulness of the threat and the asset cost. The security response link relates the security grades and policies based on the security threat. The authors have also done a simulation for the proposed model.

In (Riahi *et al.,* 2014), a cognitive approach to security systems is proposed based on the various components interacting in the IoT systems: person, intelligent object, technological ecosystem and process. The proposed model is based on the principles of trust, responsibility, privacy, safety and immunity. The model has been divided into planes namely: safety plane, access plane, cyber-security plane and the security plane, each consisting of different components and the relationship between each of the above mentioned principles. Further, the roles and needed security measures are described for each component of the IoT system. A person should be able to address, audit and implement the security practices and rules. A set of standard areas need to be kept in mind to carry out a

secure process: risk management, security, security controls implementation, security monitoring and security process monitoring and updating. A technological ecosystem should have the following security elements: security design and configuration, identification and authorization, enclave internal, enclave boundary, physical and environmental security. Each of the intelligent objects does a specific function so thereby requires security measures accordingly, example sensors.

In (Xu *et al.,* 2014), the author aims to provide an impetus for the development of IoT CAD development system. It presents the security design challenges and opportunities and hardware based IoT security approaches. Computer aided design has gone through many changes, the most recent being introduction of IoT systems. This has attracted various security metrics to be introduced. The main claim is that hardware based security approach is suitable for security requirements of IoT. They have surveyed two hardware results. Firstly, transforming several analog PUF's into stable devices. This has small hardware overhead and no delay and energy overheads. Second, digital hardware PUF security primitives initialized using stable analog PUF's. These can be used for creation of new security primitives. There are three disadvantages to using hardware primitives. Firstly, private key protocols were used until the introduction of public physical unclonable functions (PPUF) which added significant time and energy overhead. Secondly, the key based hardware PUF is unstable with respect to operational and environmental conditions such as device aging. Thirdly, the first generations of PUFs are analog circuitry. The discussion is ended with the need to search for a hardware security primitives that ensure secure data flow and prevent malicious attacks.

In (Trappe *et al.,* 2015), the authors highlight the fact that low energy devices are being used for IoT systems and the difficulty in affordable security for these devices. It highlights the viewpoint that the lower end of the IoT systems can't be secured using the present security measures and therefore more research is needed in this field. These devices require security for confidentiality, authentication, integrity, nonrepudiation and availability. As the size and energy in these devices is low, cryptographic measures are difficult to implement as they require storage space for the algorithm. This has been explained with the example of RC5 Algorithm that was popular in RFID devices for security purposes using cryptography. The proposed solution is provided based on the current available security resources. We can reuse the existing functions and thereby not giving extra energy burden on the devices.

In (Sarigiannidis *et al.,* 2015), the authors have proposed solution software VisIO T for the security of IP-enabled Wireless Sensor Network Systems (WSNs). The current security measures are based on MAC layer, network security layer issues or key management problems. The proposed tool is based on visual analytical approach, which is an integration of visual and automated data analysis. VisIO T includes a visual assisted intrusion detection system to detect complex patterns of sensor network attacks. It uses cross-free radial layout to monitor the network status and reveal sensor attacks. It consists of a planar view in the form of concentric circles to visualize the network topology. The event logger keeps track of the network events on a time adjusting basis. The VisIO T is further explained using simulations and case studies to detect and identify the root cause of several attacks.

In (Mahmoud *et al.,* 2015), a survey and analysis is presented on the current status and concerns of IoT security. It lays emphasis on the need of security measures at each layer of IoT systems: perception, network and application. It highlights the following security measures needed to be applied at each of the levels: confidentiality, integrity, availability, authentication, lightweight solutions, heterogeneity, policies and key management systems. Further the security challenges in each of the layers have been highlighted. The perception layer: strength of the wireless signal, interception of the signal from the IoT sensors and dynamic nature of IoT nodes. The Network Layer: DoS and man in the middle attacks followed by eavesdropping, confidentiality and privacy. The application layer: data privacy and identity authentication. The suggested counter measures are also suggested. Proper authentication measure like RFID, hashing and feature extraction, one time one cipher method, elliptic curve cryptographic etc. the need of trust establishment, security awareness and a federated architecture is also highlighted. It has also highlighted the future research directions namely architecture standards, identity management, session layer and 5G protocol.

**Conclusion**

All the current research workers have tried to focus on how to make the network of IoT Systems more secure from the various kinds of security threats and attacks. Each of them have tried giving an optimal solution to the particular problems that they have addressed and have also provided future work that can be carried out in that field. With the growing need of the society to move towards a fully automated environment, the data is becoming more susceptible to security threats and thereby steps are needed to be taken to resolve those. Therefore, if we apply the above mentioned solutions on the various layers and devices of the IoT system, we may create a system that is free of all kinds of security threats and attacks.

## REFERENCES

Gou, Q., Yan, L., Liu, Y. and Li, Y. 2013. Construction and strategies in IoT security system. In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing* (pp. 1129-1132).

Liu, C., Zhang, Y. and Zhang, H. 2013. A novel approach to iot security based on immunology. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on* (pp. 771-775).

Mahmoud, R., Yousuf, T., Aloul, F. and Zualkernan, I. 2015. Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp.336-341).

Premnath, S. N. and Haas, Z. J. 2015. Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model. *Wireless Communications Letters, IEEE*, *4*(3), 277-280.

Riahi, A., Natalizio, E., Challal, Y., Mitton, N. and Iera, A. 2014. A systemic and cognitive approach for IoT security.

In *Computing, Networking and Communications (ICNC), 2014 International Conference on* (pp. 183-188).

Sarigiannidis, P., Karapistoli, E. and Economides, A. A. 2015. VisIoT: A threat visualisation tool for IoT systems security. In *Communication Workshop (ICCW), 2015 IEEE International Conference on* (pp. 2633-2638).

Schurgot, M. R., Shinberg, D. A. and Greenwald, L. G. 2015. Experiments with security and privacy in IoT networks. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a* (pp. 1-6).

Tiburski, R., Amaral, L. A., Matos, E. D. and Hessel, F. 2015. The importance of a standard securit y archit ecture for SOA-based iot middleware. *Communications Magazine, IEEE*, *53*(12), 20-26.

Trappe, W., Howard, R. and Moore, R. S. 2015. Low-Energy Security: Limits and Opportunities in the Internet of Things. *IEEE Security & Privacy*, (1), 14-21.

Xu, T., Wendt, J. B. and Potkonjak, M. 2014. Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design* (pp. 417-423).

*******