Understanding, Exploring And Addressing The Security Issues In Internet Of Things (Iot): A Researcher's Perspective

[1]Binod Kumar Pattanayak, [2]Hosenkhan Reza
[1]Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, India,
Email: binodpattanayak@soa.ac.in[1]
[2]Faculty of Information and Communication technology, Universite des Mascareignes, Mauritius,
Email: rhosenkhan@udm.ac.mu[2]

Keywords: IoT, Security, privacy, vulnerability;

1. Introduction

Tehcnological innovations in the field of global data communication have been intensified over the years and consequently, the emergence of global Internet has driven the communication technology into new dimensions. Internet services have spread over a wide spectrum of areas relating to socio-economical, technological and many other professional enterprises. Seamless communications across the Internet have been the prime source of communication among the people around the globe. However, such communications have been limited to human-to-human only. A further innovation to the existing Internet has been explored wherein even device-to-device autonomous communications are made viable independent of human interventions [1]. This is referred to as Internet of Things (IoT) that is also regarded as the future Internet which connects a wide range of devices as depicted in [Fig.1]. Here, “Things” are referred to the devices connected to the IoT environment. The IoT architecture encompasses infinitely large number of autonomous smart devices. Diffrent sources in the available literature reveal that as many as 30 bilions of such devices are expected to be connected to the Internet by 2025. In IoT environment, the devices are connected to the Internet through sensing devices in order for their proper management and identification. Since most of the devices use aradio frequency based connection, each of them is associated with a Radio frequency Identifier (RFID) tag which is used for the identification purpose. This innovative technology is not only used for industrial development, but at the same time, it leaves a significant impact on the day-to-day life of people. Hence, a great emphasis is given to it by the researchers and scientists. The major application areas of IoT includes healthcare, agriculture, education, military operations, disaster recovery operations and so on [2, 3]. However, security challenges related to these these devies have become the major concern for researchers and sacientists all over the world. The heterogenity and varying architectural complexities of smart devices connected to the Internet further intensify the security challenges. In addition to this, the open inbound ports associated with each device make it even more vulnerable to security breach. The traditional security measures presumably fail comprehensively to address such security challenges that motivates novel security solutions to be innovated fo IoT devices [4]. In this paper, we have addressed various IoT security issues and challenges along with proposed measures as revealed in the available yet literature. The rest of the paper is organized as follows.

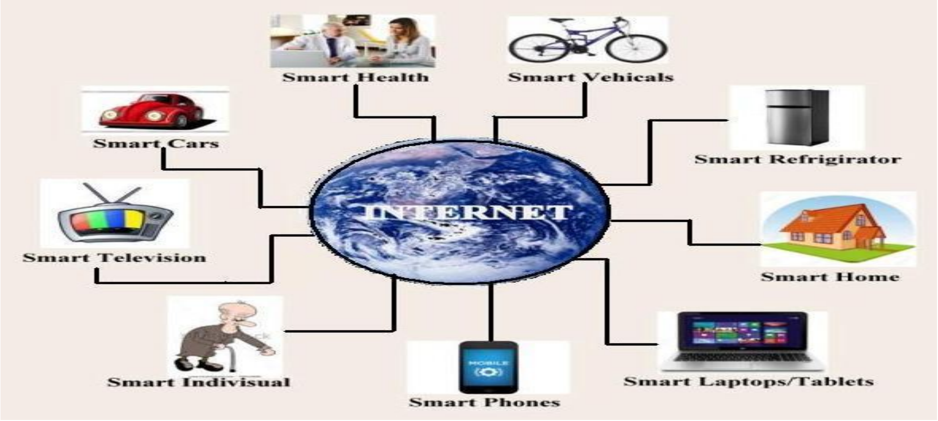
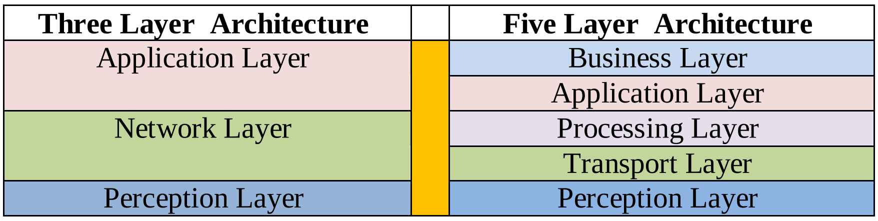


Fig.1: A High Level View of Internet of Things (IoT)

The rest of the paper is organized as follows. Section 2 describes the IoT architecture. IoT security architecture is detailed in Section 3. Security ussues and challenges pertaining to IoT environment is covered in Section 4. The related work on IoT security is included in Section 5 and Section 6 concludes the paer along with possible future extensions.

2. IoT Architecture

A thorough investigation across numerous literature on IoT, it can be observed that there is no unified consensus on the protocol architecture of IoT. We discuss here three-layer and five-layer architectures as detailed by authors in [5]. Diffrent IoT protocol layers for both of the architectures are shown in Fig.2. During the early days, a three-layer architecture for IoT was proposed that comprised of the layers such as Perception Layer, Network Layer and Application Layer. The Perception Layer was meant for performing the functions of a traditional physical layer as in any other networking protocol. The physical layer incorporates sensors to perceive the environment and gathers iformation about different parameters and also identifies other smart devices within its sensing range. The network layer is responsible for processing and transmitting the sensed by physical layer data and connecting with other devices as well. The application layer provides services to specific IoT applications such as smart city, smath home etc. However, this three-layer architecture lacks in the finer granularity of IoT technology that makes it difficult for analysis and research of IoT devices. In order to provide this granularity in understanding the IoT process, five-layer architecture was introduced that comprised of perception, thransport, processing, application and business layers. The perception, network and application layer have the significance as elaborated earlier in the context of three-layer architecture. The transport layer passes the data received from perception layer to the processing layer and vice versa using the technologies like RFID, 3G, LAN and Bluetooth etc. The processing layer is also regarded as the middleware that is responsible for storing, analyzing and processing the data received from the transport layer using databases, cloud computing technology, Big data analytics and so on. The business layer that is the uppermost layer in IoT protocol stack is solely responsible for managing the IoT system as a whole.



Three Layer Architecture		Five Layer Architecture
Application Layer		Business Layer
		Application Layer
Network Layer		Processing Layer
		Transport Layer
Perception Layer		Perception Layer

Fig.2: IoT Protocol Architecture

3. IoT Security Architecture

Security provisioning in IoT environment must be implemented at the individual layers of the protocol stack. A security architecture is depicted in Fig.3 where we have taken into consideration a three

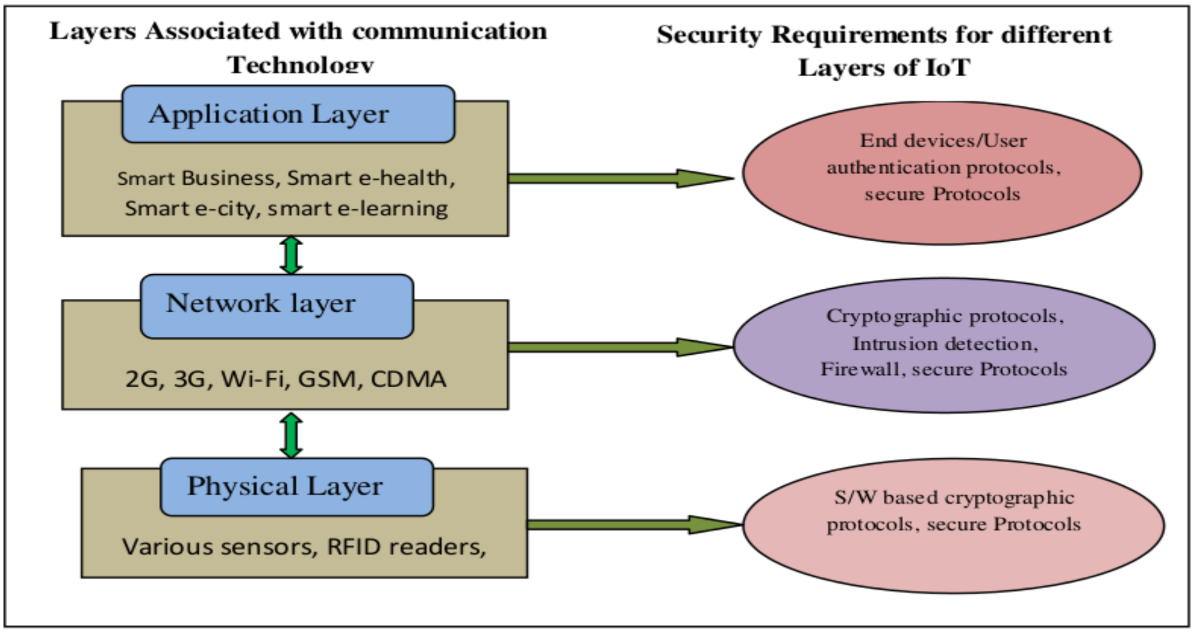

Layers Associated with communication Technology
Security Requirements for different Layers of IoT
Application Layer
Smart Business, Smart e-health, Smart e-city, smart e-learning
Network layer
2G, 3G, Wi-Fi, GSM, CDMA
Physical Layer
Various sensors, RFID readers,
End devices/User authentication protocols, secure Protocols
Cryptographic protocols, Intrusion detection, Firewall, secure Protocols
S/W based cryptographic protocols, secure Protocols

Fig.3: IoT Security Architecture

-layer IoT architecture. At the level of the physical layer, various sensors, RFID readers as well as cameras are used in order to sense the environment and record the relevant for the respective IoT application data. At this level strong authentication mechanism and privacy protection measures must be taken care of. For this purpose, various cryptographic algorithms can be used for providing data security. The network layer may use wired or wireless technologies for communication with technologies like 2G, 3G, Wi-fi, CDMA or GSM. At this layer, cryptographic protocols may be used for cloud environment to ensure data security, IPSec protocol for communication security, intrusion detection systems anf firewalls. Application layer may implement smart applications such as smart healthcare, smart busines, smart e-city, smart e-learning applications which require strong and robust authentication mechanisms which can be achieved using end device/user authentication protocols along with secure communication protocols like Constrained Application Protocol (CoAP), Near Field Communication (NFC), Long Range Wide Area Network (LoraWAN) and so on.

4. IoT Security Issues and Challenges

The heterogenity of devices connected to the IoT environment presents huge challenges for implementing security measures for efficient and secure communication among devices. Since the classes of devices on IoT may range from main frame computers to small hand-held radio frequency operated memory constrained devices, the security protoccols must be compatible with the diversity of underlying architectures across various IoT devices. Moreover, traditional network security protocols may not be capable of addressing the security aspects of IoT due to the diversity in its architectural components. Different layerwise issues and challenges pertaining to IoT technologies along with their probable solutions are listed below.

4.1. Perception Layer

The security issues relating to IoT perception layer and their measures are detailed below.

a) Unauthorized Access to the tags: Every IoT devices may be associated with a RFID tag for its unique identification in the network. Attackers may tend to delete or modify this tag which makes it impossible for the authentication of the device. In order to protect the device from attackers, cryptographic HASH Algorithm can be used to ensure the authentication of the device during communication.

b) Tag Cloning: The attackers may duplicate the tag which may lead to improper authentication at teh receiver and to avoid this issue, cryptographic HASH Algorithm can be used.

c) Eaves Dropping: The attackers may attempt to obtain access to confidential information like password which refers to a violation to data privacy and this can be avoided using cryptosystems Rivest-Shamir-Adelman (RSA), Data Encryption Standard (DES) and Blowfish.

d) Spoofing: A RFID device may tend to generate fake information which the receiver may assume the information to have come from an authentic source. The cryptosystems mentioned earlier can be useful in overcoming this issue.

e) RF Jamming: The radio frequency channel through which the device may be connected to IoT, may be jammed due to overload of noice and in order to overcome it, dynamic risk assessment method can be used.

f) Physical Damage: Hackers/attackers may physical destroy the IoT device deployed in remote areas and for protecting teh device from such damages, the device must be damage-proof packed.

4.2. Network Layer

The issues related to IoT security at the level of network layer along with their resolutions are detailed below.

a) Sybil Attack: Here, a network node may pretend its identity to other nodes which may result in communicating to an illegal node that may lead to loss of data. In order to overcome this, authentication mechanism must implement point to point encryption between communicating nodes.

b) Sinkhole Attack: This type of attack can severely harm the confidentiality and the privacy of data. In order to tackle this problem, hop-by-hop routing or source routing strategies can eb used.

c) Malicious Attack: The attacker may send malicious code to the network which may subsequently paralize the network which can be overcome with strong authentication mechanism.

4.3. Application Layer

The security issues at the level of application layer of IoT protocol stack are elaborated as follows.

a) Malicious Code Injection:

b) Denial of Service (DOS) Attack:

5. Related Work

In modern technology, application of IoT has spread over all spheres of human life. It has attracted the attention of most of the researchers in the field of global data communication. The diversity of IoT devices has significantly increased the concerns over the security of IoT devices. IoT security has been the center of attraction of most of the researchers. Here, we summarize the contributions of various authors pertaining to IoT security. A two level IoT communication security model based on a modified lightwiehgt AES approach has been proposed by the authors in [6] wherein the authors assume use of a strong authentication mechanism for exchanging the security key between the communicating IoT nodes and then using the modified lightweight AES key for exchanging the data. Implementation of Software Defined Networking (SDN) in security provisioning for IoT devices has been performed by author in [7]. Here, the author has proposed a SDN based IoT security framework which successfully uses the intelligent networking paradigm of SDN in order to provide secure routing among IoT devices. An integration of IoT and cloud computing technologies is discussed by the authors in [8] wherein main focus is given on the security aspects of such an integration of the two emerging technologies. In a comprehensive survey presented by the authors here, the improvement of IoT functionality by virtue of ist integration with cloud computing paradigm has been addressed. A lightweight communication protocol called AccessAuth has been proposed by authors in [9] that aims at security provisioning for Vehicle-to-Grid (V2G) systems that are promoted by federated IoT technology using a capacity-aware authentication mechanism. As claimed by the authors, the optimal number of allowable access requests in a V2G domain can be computed taking into consideration the capacity limitations of the network and the mobility of the vehicles. An automatic agent trust model has been proposed by authors in [10] which addresses decreasing security concerns, increasing credibility as well reliability, ensuring information collection in dynamic IoT systems. Here authors claim that agents along with the agent platforms are necessary for all nodes in the network in order to build a credibility protection model. Such agent based nodes in an IoT system self-governing software and hardware integrated independent systems. A new security architecture IoT systems has been proposed by the authors in [11] that relies on software defined networking (SDN) concepts. Authors claim it to be a SDN-domain that can function with or without infrastructure. Authors have claimed their proposed SDN based architecture to work more efficiently as compared to other IoT security architectures. Existing issues in security as well as privacy in Internet of Things, cloud computing (CC) and cloud of things (COT) have been broadly addressed by the authors in [12]. Here, the authors have mainly focused on the confidentiality issues. Nevertheless, the issues of intriusions along with vulnerabilities remain untouched in this work. Authors in [13] address a global strategy for design of secure IoT systems that include safe solutions for environments with rich information, ensuring the devices to fucntion as desired by the manufacturer, secure life style for networks, devices as well as the data centers, supporting interoperability and industry standards of the devices and secure clouds for traditional systems. An innovative IoT security system has been proposed by the authors in [14] that protects IoT resources as well as data from the hackers. Simulation results as claimed by the authors justify the robustness as well as the ffectiveness in protecting IoT resources. A comprehensive analysis of IoT security threats has been carried out by the authors in [15] along with possible countermeasures and at the same time, a focus has been made on the aspects of encryption of IoT data in order to protect it from harmful elements. A universal two-level IoT security architecture that is integrated with the necessary security measures has been proposed by the authors in [16] that mostly focuses on inherent openness, heterogeneity and terminal vulnerability of IoT infrastucture. A PFU-based hardware security solution for IoT devices has been addressed by the authors in [17] that focuses on energy-constrained IoT devices and their security challenges. Based on an Ubiquitous to IoT model (U2IoT), a cyber-physical-social based security architecture (IPM) has been proposed by the authors in [18] that mainly focuses on security model that incorporates mapping of U2IoT, physical security in external context and the inherent infrastructure, and security strategies for social management control, that effectively addresses the security and privacy concerns of IoT environment. A game theoretic anoimaly detection technique has been propsed by the authors in [19] that is triggered on occurrence of a new attack's signature thereby achieving a balnce between detection and false positive rates as well as energy consumption. Here, in order to reduce the false positive rate, a game theoretic reputation model has been proposed. As claimed by the authors, the simulation results prove its better performance as compared to other existing anomaly detection techniques. Transmission efficiency of business information along with improved application data security has been addressed by the author in [20] that relies on custom data packet encapsulation technique thereby reducing the overhead of data resources combined with secure encryption and decryption techniques.

6. Conclusion and Future Work

Internet of Things has become extremely popular among the researchers around the globe over the recent years. Implemetation of IoT applications has been enormous due to its diversified somain of application. However, successful implemenation of IoT technology faces a series of issues and chjallenges esp[ecially in the context of network security. A broad spectrum of research work is available in the literature for addressing these issues. In this paper, we have made an attempt to review these security issues and challenges, their probable resolutions comprehensively. Nevertheless, the domain of IoT security is vast and needs a lot of attention. In future, we wish to carry out our work on IoT security in a more focused manner.

Reference

1. Bhabad M. A. and Bagade S. T., Internet of Things: Architecture, Security Issues and Countermeasures, International Journal of Computer Applications (IJCA), Vol.125, No.14, pp.1-4, 2015.
2. Ramlowat D. D. and Pattanayak B. K., Exploring Internet of Things (IoT) in Education: A Review,
3. Rath M. and Pattanayak B. K., Technological Improvement in Modern Health Care Applications Using Internet of Things (IoT) and Proposal of Novel Health Care Approach,

4. Hosenkhan R. and Pattanayak B. K., A Secure Communication Model for IoT,
5. Sethi P. and Sarangi S. R., Internet of Things: Architectures, Protocols and Applications, Journal of Electrical and Computer Engineering (JECE), pp.1-26, 2017.
6. Pattanayak B. K. and Amic S., Modified Lightweight Based two level Security Model for Communication on IoT, TEST Engineering and Management, Vol.82, No.1-2, pp.2323-2330, 2020.
7. Vandana C. P., Security Improvement in IoT based on Software Defined Networking (SDN), International Journal of Science and Technology Research (IJSTR), Vol.5, No.1, pp.291-295, 2016.
8. Stergiou C., Psannis K. E., Kim B. G. and Gupta B., Secure Integration of IoT and Cloud Computing, Future Generation Computer Systems, Vol.78, pp.964-975, 2018.
9. Tao M., Ota K., Dong M. and Qian Z., AccessAuth: Capacity-aware Security Access Authentication in Federated-IoT-Enabled V2G Networks,
10. Procedia Computer Science, Vol.21, pp.107-113, 2013.
11. Oliver F., Carlos G. and Florent N., New Security Architecture for IoT Network, Procedia Computer Science, Vol.52, pp.1028-1033,
12. Sahmim S. and Gharsellaoui H., Privacy and Security in Internet-Based Computing: Cloud Computing, Internet of Things and Cloud of Things: A Review, Procedia Computer Science, Vol.112, pp.1516-1522, 2017.
13. Tedeschi S., Mehnen J., Tapoglou N. and Roy, R., Secure IoT devices for the maintenance of machine tools. In *Procedia Cirp* (Vol. 59, pp. 150-155). Elsevier, 2017.
14. Said O., Development of an Innovative Internet of Things Security System, International Journal of Computer Science Issues (IJCSI), Vol.10, Issue 6, No.2, pp.155-161, 2013.
15. Ahmed A. W., Ahmed M. M., Khan M. A. and Shah O. A., A Comprehensive Analysis on the Security Threats and Their Countermeasures of IoT, International Journal of Advanced Computer Scienc and Applications (IJSACSA), Vol.8, No.7, pp.489-501, 2017.
16. Zhang W. and Qu B., Security Architecture of the Internet of Things Oriented to Perceptual Layer, International Journal on Computer, Consumer and Control (IJ3C), Vol.2, No.2, pp.37-45, 2013.
17. Halak B., Zwolinski M. and Mispan M. S., Overview of PFU-Based Hardware Security Solutions for the Internet of Things, Proceedings of the IEEE 59th International Midwest Symposium on Circuits and Systems (MESCAS), 2016.
18. Ning H. and Liu H., Cyber-Physical-Social Based Security Architecture for Future Internet of Things, Advances in Internet of Things, Vol.2, pp.1-7, 2012.
19. Sadjelmaci H., Senouci S. M. and Taleb T., An Accurate Security Game for Low-Resource IoT Devices, IEEE Transactions on Vehicular Technology. Vol.66, No.10, pp.981-993, 2017.
20. Yanling Z., Research on Data Security Technology in Internet of Things, Applied Mechanics and Materials, Vol.433-435, pp.1752-1756, 2013.