Volume 5, Issue 11, November 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An analysis of Security Issues of Internet of Things (IoT)

[1]Eeshan Pandey[*], [2]Varshi Gupta

[1]Department of Computer Science & Engineering, Sir Padampat Singhania University, Bhatewar, Rajasthan, India

[2]Associate Software Engineer Accenture, India

Abstract*— Nowadays, more than two billion people around the world use Internet for browsing the web, sending and receiving emails, using multimedia content and services, playing games, using social networking applications and several different. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, compute and coordinate. It is predictable that, within the next decade, the Internet will exist as a seamless fabric of classic networks and networked objects. Content and services will be all around us, always available, paving the way to new applications, enabling new ways of working; new ways of interacting; new ways of entertainment; new ways of living. Security is thus a major concern for the developing field such as IoT. Keeping that in mind this paper will discuss major security concerns and how to overcome them using various algorithms.

***Keywords*— Internet of Things, IoT, IoT security goals, IoT security challenges and issues, IoT security architecture.**

I. INTRODUCTION

Internet of Things, a consolidated system of interconnected devices and networks, was proposed by Kevin Ashton in the year 1999 [1]. It can be coined as a revolution that has updated the existing Internet infrastructure to a concept of a level up advanced computing network where all the physical objects around us will be connected to each other and will be uniquely identified [2]. By this continuously emerging technology everything around us like mobile phones, cars, watches, accessories etc will be collecting some useful user data with the help of various technologies, and will pass on the data to a well-defined ecosystem in which the collected data will be used to perform different tasks autonomously.

A large number of researches are occurring and the vision of IoT will soon become a reality. According to Gartner, more than 25 billion uniquely identifiable objects are expected to be a part of this global computing network by the year 2020 [3], which is a giant figure on papers and on reality, however when such a big network of interconnected devices will prevail there will be some new security and privacy issues and all the interconnected devices will be exposed to a high risk of hackers as they clutch at the security gaps to make the devices work as per their wish. IoT is highly flexible and robust and promises a high end futuristic scope but it has a high potential of security disaster also. There are many discussions on its adoption on a high scale, but without successfully solving the prevailing security threats, it does not seem to have any future [4]. Due to easy access to the objects, it can be easily exploited by the hackers at any point of time [5]. No matter how much secure companies think their products are, they are still prone to various kinds of attacks so they must ensure that the patches are made available as and when any vulnerability is detected in the system. Since the devices are directly connected to the users' day to day life so security considerations must be the highest priority and there must be some proper well-defined security infrastructure to limit the threats related to robustness, availability and security of IoT [6]. The paper is organized as follows. Section 2 describes the generic architecture of IoT. Section 3 describes the security goals. Section 4 discusses the major security challenges and issues on each layer. Section 5 presents the security architecture of IoT and finally Section 6 concludes the paper.

II. GENERIC ARCHITECTURE

Generally, IoT has four main key levels as shown in Fig. 1, which are described below [7]:

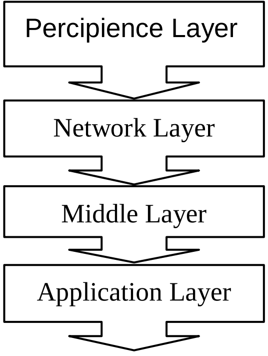

Fig. 1 Main key levels of IoT

A. Percipience Layer

Percipience layer consists of different kinds of data sensors like RFID, Barcodes or any other sensor network [8]. The basic purpose of this layer is to identify the unique objects and deal with its collected data obtained from the real world with the help of its respective sensor(s).

B. Network Layer

The purpose of this layer is to transmit the gathered information obtained from the perception layer, to any particular information processing system through existing communication networks like Internet, Mobile Network or any other kind of reliable network [9].

C. Middle-ware Layer

This layer consists of information processing systems that take automated actions based on the results of processed data and links the system with the database which provides storage capabilities to the collected data. This layer is service-oriented which ensures same service type between the connected devices [10].

D. Application Layer

This layer realizes various practical applications of IoT based on the needs of users and different kinds of industries such as Smart Home, Smart Environment, Smart Transportation and Smart Hospital etc [11].

III. SECURITY GOALS

The major security goals of IoT are to ensure proper identity authentication mechanisms and provide confidentiality about the data etc. The information security triad, a distinguished model for the development of security mechanisms, implements the security by using CIA which is Data Confidentiality, Integrity and Availability as shown in the Fig. 2. A breach in any of these areas could cause serious issues to the system so they must be accounted for. The three areas are described below:

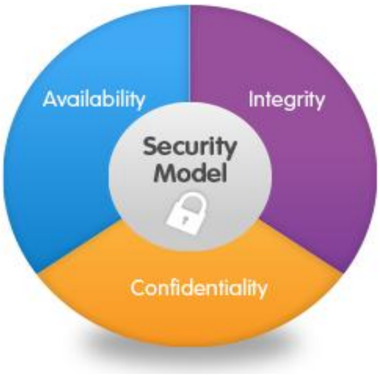

Fig. 2. The CIA Triad

A. Data Confidentiality

Data confidentiality refers to the ability to ensure privacy for the user by using different mechanisms such that its disclosure to the unauthorized party is prevented and can be accessed by the permitted users only. There are many security mechanisms to provide confidentiality of the data including Data Encryption in which the data is converted into cipher text which makes it difficult for the unauthorized person to use it and the Two-step verification, which provides authentication by two dependent components and allows the access only if both the components pass the authentication test and the most common Biometric Verification in which every person is uniquely identifiable. For the IoT based devices, it ensures that the sensor nodes of the sensor networks don’t reveal their data to the neighbouring nodes; similarly the tags don’t transmit their data to an unauthorized reader [12].

B. Data Integrity

Data Integrity refers to the protection of useful information from the cybercriminals or the external physical interference during communication with some common tracking methods, so that the data tampering cannot be done without the system catching the threat [13]. The methods to ensure the accuracy and originality of data include methods like Checksum and Cyclic Redundancy Check (CRC) which are simple error detector mechanisms for a portion of data. Moreover, continuous syncing of the data for backup purposes and the feature like Version control, which keeps a record of the file changes in a system to restore the file in case of fortuitous deletion of data can also ensure the integrity of data such that the data on IoT based devices is in its original form when accessed by the permitted users.

C. Data Availability

One of the major goals of IoT security is to make data available to its users, whenever needed. Data Availability ensures the immediate access of authorized party to their information resources not only in the normal conditions but also in disastrous conditions. Due to dependency of companies on it, it is necessary to provide firewalls to countermeasure the attacks on the services like Denial-of-service (DoS) attack which can deny the availability of data to the user-end. Data

Availability also ensures the prevention of bottleneck situations which prevent the flow of information. The Redundancy and Failover backup methods provide duplication of the system components in conditions of system failure or various system conflictions to ensure reliability and availability of data.

IV. SECURITY CHALLENGES AND ISSUES

There have been many accomplishments in the research field of IoT, however there are still many open challenges which needs to be addressed for the uniqueness of this technology. In this section some of the threats which need special attention are discussed below for each architectural layer.

A. Perception Layer Challenges

Perception layer contains various sensor technologies like RFID which might be exposed to many kinds of threats that are discussed below:

1) *Unauthorized Access to the Tags:* In a large number of RFID systems, lack of proper authentication mechanisms can lead to someone accessing the tags without authorization. The attacker can not only read the data but can modify or delete it as well [14].
2) *Tag Cloning:* Tags can easily be captured by cyber criminals since they are deployed on different objects which are visible and their data can be read and modified with some hacking techniques .These miscreants can create a replica of the tag and hence compromise it in a way that the reader cannot differentiate between the original and the compromised tag [15].
3) *Eavesdropping:* Wireless nature of the RFID makes it very easy for the attacker to sniff out the confidential information like passwords or any other data transfer from tag-to-reader or reader-to-tag which endangers it because the attacker can make use of it in despicable ways [16].
4) *Spoofing:* Spoofing is when attacker broadcasts fake information to the RFID systems which assume it is coming from the original source [17]. This way attacker gets full access to the system making it vulnerable.
5) *RF Jamming:* RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is blocked with an overload of noise signals [18].

B. Network Layer Challenges

Network layer subsists of the Wireless Sensor Network (WSN) which transfers the data from the sensor to its destination with reliability. Following are the related security issues:

1) *Sybil Attack:* Sybil is a kind of attack in which the attacker manoeuvres the node to show multiple identities for a single node which compromises a considerable part of the system resulting in false information about the redundancy [19].
2) *Sinkhole Attack:* It is a kind of attack in which the miscreant makes the compromised node look alluring to the nearby nodes due to which all the data flow from neighbouring nodes is shifted towards the compromised node resulting in a drop in packets i.e. the system is bamboozled to believe that the data has been received on the other side while all the traffic is silenced. Moreover this attack results in more energy consumption which can cause DoS attack [20].
3) *Sleep Deprivation Attack:* The sensor nodes follow sleep routines to extend their lifetime since WSNs are powered with batteries with poor lifetimes. Sleep Deprivation is the kind of attack which keeps the nodes awake anyhow, resulting in more battery consumption and as a result battery lifetime is reduced which causes the nodes to shut down [21].
4) *Denial of Service (DoS) Attack:* The kind of attack in which the network is overloaded with a useless lot of traffic by an adversary, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users [22].
5) *Malicious code injection:* This is a serious kind of attack in which an attacker injects a malicious code into the system to compromise a node that could even result in a complete shutdown of the network or in the worst case, the attacker can get a full control of the network [23].
6) *Man-in-the-Middle Attack:* This is a form of Eavesdropping in which target of the attack is the communication channel due to which the unauthorized attackers can monitor or control all the private communications between the two nodes hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information [24].

C. Middle-ware Layer Challenges

This layer is composed of data storage technologies like cloud computing. The security challenges faced in this layer are given below:

1) *Unauthorized Access:* Middle-ware Layer provides data storage facilities and various interfaces for the applications. The adversary can endanger the system by restricting the access to the related services of IoT or by removing the existing data. So an unauthorized access could be cataclysmic for the system.
2) *DoS Attack:* It is similar to the DoS attack given in the previous two layers i.e. it shuts down the system which results in unavailability of the services.
3) *Malicious Insider*: This kind of attack happens when a person from the inside meddles the data for personal benefits or for any third party. The data can be easily read and then changed on purpose from the inside.

D. Application Layer Challenges

The related security issues of this layer are described below:

1) *Malicious Code Injection:* Using some hacking techniques an adversary can inject any kind of malicious code to leverage an attack on the system from end-user and steal some kind of data from the user.
2) *Denial-of-Service (DoS) Attack*: DoS attacks nowadays have become sophisticated, they offer a smoke screen while attacks to breach the defensive system and data privacy of the user, deceiving the victim into believing that the actual attack is occurring someplace else. This puts the non-encrypted personal details of the user at the hands of the hacker.
3) *Spear-Phishing Attack:* It is an email spoofing attack in which victim, a high ranking person, is lured into opening the email through which the attacker gains access to the credentials of that victim and then by a faked pretense extracts highly sensitive information.
4) *Sniffing Attack:* An attacker can introduce a sniffer application in the system to force an attack on it, which could gain network information resulting in corrupted system [25].

V. SECURITY AT DIFFERENT LAYERS

Confidentiality of data and privacy being the primary concern these days there are many researches being carried out in this direction to provide a reliable well-defined security architecture which can ensure data security. W. Zhang et al. [26] proposed architecture for the security against the possible threats, as shown in Fig. 3.

A. Perception Layer

Perception Layer is the last layer of the IoT architecture which assigns many security features to the hardware. It serves four basic objectives i.e. Authentication, Data Privacy, Privacy of sensitive information and Risk Assessment which are defined below:

1) *Authentication:* Cryptographic Hash Algorithms that provide digital signatures to the terminals which could resist all the probable known attacks like Collision attack, Side-channel attack, Brute force attack etc. are used to do authentication.
2) *Data Privacy:* Privacy of the data is ensured by asymmetric and symmetric data encryption algorithms such as BLOWFISH, RSA, DES etc. These algorithms prevent an unauthorized access to the sensitive data in the duration of being gathered or delivered to the next layer. Since they consume less power it is beneficial to implement them into the sensors.
3) *Privacy of sensitive information:* As for shielding the sensitive information, K-Anonymity approach is used which ensures anonymity of the location and identity of the user. This approach is helpful in keeping user location out of reach of malicious attacks [27].
4) *Risk Assessment:* Risk Assessment is indispensable for IoT security as it helps in discovering the new threats to the system. It helps in analysing optimum security strategies and defending the security breaches. For example Dynamical Risk Assessment method which is continuous process of identifying hazards and assessing risk can be used for risk monitoring [28]. Even after employing such security measures, if an intrusion is found in the system, an built-in Kill-command from the RFID reader is sent to the RFID tag to prevent unauthorized access to data [29].

B. Network Layer

The network layer, either wired or wireless is exposed to different kinds of cyber attacks. Hackers these days are able to monitor communications easily due to the openness of the wireless channels. Following are the types of the network layer security:

1) *Authentication:* Illegal access to sensor nodes to circulate untrue information can be prevented with the help of a proper authentication process and point to point encryption [30]. The commonest of all attacks is DoS attack that influences the network by sending a lot of futile traffic towards it by a number of botnets powered by the system of interconnected devices.
2) *Routing Security:* After the Authentication process, we use routing algorithms to guarantee the safety of data transfer among the sensor nodes and the processing systems [31]. A multitude of researches have been carried out in this direction for finding the routing ways including “Hop-by Hop Routing” in which only address of the data destination is known. Also, the “Source Routing” [32], where data to be transmitted is stored in the form of packets which are then analyzed by the intermediate nodes and finally sent to the processing system. Multiple paths for the data routing enhance the security of routing and improve the ability of the system to find a bug and keep performing even after any kind system failure [33].
3) *Data Privacy:* The safety control mechanisms checks the system for any kind of intrusion and finally Data integrity methods are implemented to make it certain that the data received on the other end is congruous to the original one.

C. Middle-ware and Application Layer

This layer merges the Application and Middle-ware layer to form an integrated security mechanism. The security categories are mentioned below:

1) *Authentication:* Initially the access to any malicious user is restricted through the authentication process which defends by integrated identity identifications. This is completely similar to that of the identification process in either of the layers except that this layer instigates authentications by certain cooperating services which basically means that users can even pick the correlated information to be shared with the services. Cloud computing and Virtualization are the main technologies which are used in this layer, both of which can easily be subjected to various attacks. Insider threats are the most feared for the cloud technology. Similarly, virtualization is endangered by DOS and data theft etc. A lot of research is required for providing a secure environment in both the technologies.
2) *Intrusion Detection:* Intrusion detection techniques generate an alarm on occurrence of any suspicious activity in the system and administer solutions for various security threats by the uninterrupted monitoring and maintaining a log of the intruder's activities that helps in tracing the intruder. There are various extant intrusion detection techniques [34] including the data mining approach [35] and anomaly detection.
3) *Risk Assessment:* The risk assessment provides rationalization for the adequate security strategies and helps in foreseeing enhancements in the already existing security structure.
4) *Data Security:* Different encryption technologies assure data security and prevent the data pilfering threats. AntiDos Firewalls and other spywares have been introduced just to prevent such malicious activities from miscreant users.

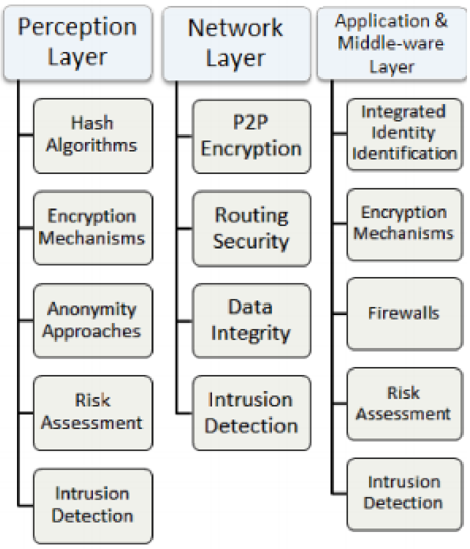

Fig. 3. Security Architecture of IoT

VI. CONCLUSION

Data security and trusted privacy are the only hurdles that stand in the path of further IoT development. Security at all the levels of IoT is mandatory for the proper functioning of IoT. To date, there already have been many research accomplishments which dilute IT security concerns and achieve effective implementation of a security infrastructure for IoT. These research parameters need to be expanded further and focus the attention towards looking for new possible security solutions, so as to make IoT able to block adversaries and provide secure services to the coming generation of data-hungry billions of devices. Efficient privacy and security measures through fundamental research must be found out and the open questions in this research field must be answered, before it is a part of society. This paper talked about the security goals and probable security challenges and problems of the IoT system. In the future, more authentications, risk assessment and intrusion detection techniques in each architectural layer must be explored hand in hand with the implementation of the security infrastructure using extant IT security features. Moreover, legal frameworks, proper regulations and policies must be made to assure steady development of the secure technologies.

ACKNOWLEDGMENT

We wish to acknowledge our friends and family for their support, guidance and help which was a consistent source of motivation.

REFERENCES

[1] Kevin Ashton, *That Internet of things*, It can be accessed at: http://www.rfidjournal.com/articles/view?4986

[2] D. Singh, G. Tripathi, A.J. Jara, *A survey of Internet-of Things: Future Vision*, Architecture, Challenges and Services, in Internet of Things (WF-IoT), 2014

[3] Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717

[4] Rolf H. Weber, *Internet of Things - New security and privacy challenges* in Computer Law and Security Review (CLSR), 2010, pp. 23-30

[5] Rodrigo Roman, Pablo Najera and Javier Lopez, *Securing the Internet of Things* in IEEE Computer, Volume 44, Number 9, 2011, pp. 51-58

[6] Friedemann Mattern and Christian Floerkemeier, *From the Internet of Computers to the Internet of Things,* in Lecture Notes In Computer Science (LNCS), Volume 6462, 2010, pp 242-259

[7] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, *Security in the Internet of Things: A Review*, in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651

[8] Ying Zhang, Technology Framework of the Internet of Things and Its Application, in Electrical and Control Engineering (ICECE), pp. 4109-4112

[9] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, A Multilayer Security Model for Internet of Things, in *Communications in Computer and Information Science, 2012, Volume 312*, pp 388-393

[10] Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, *Future Internet: The Internet of Things Architecture*, Possible Applications and Key Challenges, in 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, pp. 257-260

[11] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013

[12] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac,*Internet of Things: Vision, applications and research challenges,* in Ad Hoc Networks, 2012, pp.1497-1516

[13] Luigi Atzori, Antonio Iera, Giacomo Morabito, *The Internet of Things: A Survey,* in Computer Networks, pp. 2787-2805

[14] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, *Internet of Things: Architecture and Security,* in International Journal of Computer Application, Volume 3, Issue 4, 2014

[15] Mike Burmester and Breno de Medeiros, *RFID Security: Attacks, Countermeasures and Challenges.*

[16] Benjamin Khoo, *RFID as an Enabler of the Internet of Things: Issues of Security and Privacy,* in IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011

[17] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, *Classification of RFID Attacks.*

[18] Lan Li, *Study on Security Architecture in the Internet of Things,* in International Conference on Measurement, Information and Control (MIC), 2012

[19] John R. Douceur, *The Sybil Attack,* in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260 [20] Nadeem AHmed, Salil S. Kanhere and Sanjay Jha,*The Holes Problem in Wireless Sensor Network: A Survey,* in Mobile Computing and Communications Review, Volume 1, Number 2

[21] Tapalina Bhattasali, Rituparna Chaki and Sugata Sanyal, *Sleep Deprivation Attack Detection in Wireless Sensor Network,* in International Journal of Computer Applications, Volume 40, Number 15, 2012

[22] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, *A survey of ATtacks, Security Mechanisms and Challenges in Wireless Sensor Networks*, in International Journal of Computer Science and Information Security, Volume 4, Number 1, 2009

[23] Priyanka S. Fulare and Nikita Chavhan, *False Data Detection in Wireless Sensor Network with Secure Communication,* in International Journal of Smart Sensors and AdHoc Networks (IJSSAN), Volume-1, Issue-1, 2011

[24] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, *Cloud Computing: Security Issues and Research Challenges,* in International Journal of Computer Science and Information Technology & Security (IJCSITS).

[25] Bhupendra Singh Thakur, Sapna Chaudhary, *Content Sniffing Attack Detection in Client and Server Side: A Survey,* in International Journal of Advanced Computer Research, Volume 3, Number 2, 2013

[26] W. Zhang, B. Qu, *Security Architecture of the Internet of Things Oriented to Perceptual Layer,* in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2 (2013)

[27] K.E. Emam, F.K. Dankar, *Protecting Privacy Using Anonymity,* in Journal of the American Medical Informatics Association, Volume 15, Number 5, 2008

[28] C. Liu, Y. Zhang, J. Zeng, L. Peng, R. Chen, *Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology,* in Eighth International Conference on Natural Computation (ICNC), 2012

[29] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, *Guidelines for Securing Radio Frequency Identification (RFID) Systems,* in Recommendations of National Institute of Standards and Technology