ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey on IoT Security Threats and Solutions

Jaychand [1], Nishant Behar[2]

Student, Dept. of C.S.E, Institute of Technology Guru Ghasidas University, Bilaspur, Chhattisgarh, India[1]

Assistant Professor, Dept. of C.S.E, Institute of Technology Guru Ghasidas University, Bilaspur, Chhattisgarh, India[2]

ABSTRACT: The Internet of Things gives a technologically optimistic view of the future where most of the objects will make intelligent communications with each other through the internet anywhere anytime .Although it really makes really appreciable progress in this field, there still uncertainties lingers with its security concepts of its usage which is still date the major topic of concern in the design of IoT architectures. This paper portrays a general survey of all the security issues in the field of IoT along with the analysis of the various architecture of IoT. The study defines various security measures, its requirements and the challenges that come along with the implementation of IoT. We discuss security threats and the solutions related to it on each layer of the IoT architecture to make this technology more secure and popular and spread it globally.

KEYWORDS: IoT security, IoT threats, IoT security solution, security solution,

I. INTRODUCTION

Internet of Things is defined by Oxford as “A proposed development of the internet in which everyday object have network connectivity, allowing them to send and receive data.”

IoT is a system that provides connectivity and interactive communication to anything. Although the term “being connected” is commonly used in electronic devices in day to day life, physical objects (i.e. hardwares) such as actuators, sensors, etc are connected with single address of the internet protocol. The wires connection or the wireless connection of the network data is consciously transmitted through the hardware to interpret. Because of the property to communicate and sense physical objects can understand the complications of the surroundings and react. These physical objects have been set up and accepted extensively and they are working appropriately without the involvement of humans. In near future, it is estimated that every day to day object will be a part of Internet. Mobile phones and similar devices will act as remote control to objects in the world and usually called as IoT. According to Gartner, the number of devices that are connected to internet is expected to rise from 25 billion to 50 billion near 2020. The rising popularity of the network leads to new risks of security and the attackers can take even more private information of the users/organizations which are associated with that IoT system. The main purpose of this thesis is to highlight the security concerns in IoT environment.

Security issues are important for IoT tools due to following reasons:
• IoT is considered as an upgraded version of a number of different technologies like Mobile Broadband, WSN (Wireless Sensor Networks) and 2G communication or 3G communications Networks and so it is probable that IoT will be under same threats in which they are already because of security flaws.
• In IoT every device is linked to Internet which is naturally not a secure environment. There are many people out there for the various system breaks and ready to execute their malware remotely.
• In IoT objects talk to each other; so, there can be a possibility of hindering the privacy and security.
This study is a survey on the security matters in IoT. The thesis describes the requirements and challenges of security that are commonly faced by IoT system in implementations. This also specifies threats and solutions of security for each layer of IoT architecture which make it more secure and widespread. In this research paper, second section describes the security requirements and challenges. Section 3 gives the details about the security threats in IoT. The

DOI: 10.15680/IJIRCCE.2017. 05032281

fourth section gives the recommended solutions for security in IoT. And the fifth section gives the summary of the IoT threats and solution in Table 1. The sixth section is the conclusion part.

II. SECURITY REQUIREMENTS AND CHALLENGES

With various equivalent technologies such as mobile networks, traditional Internet, sensor networks etc, the term ‘internet’ is extended by IoT. Anything “thing” can be connected to Internet and they can talk to each other. Although these types of systems entail high potential for scalability and flexibility, they are not free from the risk to security problems. There are lots of issues regarding their wide implementation and no significant solutions to new threats; it looks like an impractical technology for the near future.

II.1. SECURITY CHALLENGES

Interoperability: The functionality of various interconnected devices should not be prevented by relevant security solutions in IoT network system.

Resource constraints: We are not able to apply some security measures such as public key encryption algorithm and frequency hopping communication because many of the nodes in IoT architecture lack in power, storage capacity, bandwidth and CPU which makes the setup of security system very complicated.

Data volumes: Some IoT applications make use of communication channels briefly and infrequently but there are lot of IoT systems that have potentials to occupy huge amount of data on servers they are logistics, sensor-based and large size system.

Privacy protection: As there are so many RFID systems that have some sort of appropriate authentication mechanism with which anybody can follow tags and find the host’s identity. Intruders not just read data, but are able to modify or delete the data also.

Scalability: Large numbers of nodes are there in an IoT network. So a scalable security mechanism should be proposed on IoT.

Autonomic control: For configuration and adaptations in traditional computers to different application areas and in different communication situation users are required. However, connection establishment of devices in IoT network must be spontaneous and can configure themselves to get used to the operating platform. Some techniques and mechanisms are involved for this kind of control self-management, self-configuring, self-healing, self-protecting and self-optimizing.

II.2 SECURITY REQUIREMENTS

Authenticity: Illegal users are not allowed to access the sensitive information or system.

Authorization: The rights to the components of devices and it applications must be limited so that they can only access the resources needed by them to perform their tasks.

Availability and Continuity: The provision of security check should be ensured in order to avoid any possible interruptions and operational failures.

Confidentiality: Transmission of information among the nodes must be protected from impostor.

Integrity: Tampering of related data must not be there.

III. Security Threats in IoT Systems

Existing security threats of IoT system are checked in four headings on the basis of IoT architecture.

III.1. THREATS OF APPLICATION LAYER

In application layer the custom made services based on the user requirements are included; e.g. the users interface to control devices in IoT. Threats in this layer are mentioned below:

Sniffer /Loggers: Sniffer/logger programs can be introduced into the system by attackers to get important information from the network traffic. The sniffer takes any kind of passwords, files (FTP files, E-mail files), and reads E-mail text. Many protocols are vulnerable to sniffing.

Injection: Attackers may inject code directly into the application which is executed on the server. This is a very common attack, easy to use, and can cause some terrible results such as loss of data, corruption of data and lack of accountability.

Session Hijacking: In this attack personal identity is revealed by taking advantage of security flaws in authentication and session management. This sort of attack is very common and effects of attack are really significant. With someone else identity the attacker can do anything that the real user can do.

Distributed Denial of Service (DDoS): It is a type of attack where multiple system which are infected are used to cause harm to a single system .It traditional Denial of Service attack though it is executed by many individuals at the time.

Social Engineering: It is a threat to the application layer where the attackers can gain data and information from users by knowing each other, via chats, etc.

III.2. THREATS OF SUPPORT LAYER

Threats in support layer are mainly targets data storage technologies. These threats are discussed below:

Data Tampering: This attack is basically causing damage to the data by the unauthorized insider for commercial benefits of any third party companies or personal benefits. On purpose the data can be extracted and easily modified from inside.

DoS Attack: Same as DoS attacks effects seen in previous layers that it makes the service unavailable by shutting down the system.

Unauthorized Access: It is the usage of the system without any permission .An unauthorized access can be deadly as it enables the attacker penetrate into the system and damage the system by deleting important data or preventing the access to the related services of IoT without any difficulty.

III.3. THREATS OF NETWORK LAYER

Following are some threats of network layer:

Selective Forwarding: In this attack, some of the messages are not forwarded by malicious node and selectively drop them, ensuring that later they cannot propagate. The person who is responsible for modification or suppression of packets comes from a few selected nodes and sometimes forwards the remaining traffic not to reveal their illegal activity. There are different types of selective forwarding attacks. In first type, the malicious node can selectively drop the packets coming from a particular node or a group of nodes. This situation shows a risk of DoS attack for that node or a group of nodes. Its second type is called Neglect and Greed. In such type of attack, the corrupted node arbitrarily skips routing some messages.

Sybil Attack: The Sybil attack in computer security is an attack by an attacker wherein a reputation system is subverted by forging identified in peer-to-peer networks it can be in more than one place at once as a single malicious node. The device illegitimately takes on multiple identities; it is making clear as a malicious device. It gives multiple identities to other nodes in the network which reduces the effectiveness of fault tolerant schemes.

Blackhole Attack (Sinkhole): The sink hole is the intense resource conflict among the malicious node and its neighbouring nodes for the limited bandwidth and channel access. It results in congestion and can accelerate the energy consumption of the involved nodes. Its appearance in a sensor network is vulnerable to several other types of DoS attacks.

Wormhole: It’s a form of DoS attack the attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally, this means relocation of bits of data in the network. Tunnelling of bits of data is use for this relocation.

Man-in -the -Middle Attack: It’s a form of eavesdropping attack that occurs when a malicious actor monitors or controls all the confidential communications between the two systems. The attacker can even fake the identity of the victim and normally communicate to gain more information.

Hello -flood Attack: The main disrupting effect of this attack is high traffic in channels which congests the channel by sending an unusually high number of useless messages. To create a high traffic the useless message from the malicious node is replied by the attacker.

Acknowledgement Flooding: These are the algorithms for routing in sensor-based system which requires acknowledgements from time to time. In this sort of DoS attack, with the help of these acknowledgements a malicious node sends false information to destined neighbouring nodes.

III.4. THREATS OF PERCEPTION LAYER

Intelligence embedded technologies and sensor including sensors, RFID readers or GPS comes under perception layer. These are in threat because of a variety of security faults. Following are the some important threats of this layer.

Spoofing: In this the attacker initially sends a fake relay message to network as a result of which the node falsely takes its identity and make it appear from original source [29]. It is quite often that the attacker obtains full access to the system in this scenario resulting it vulnerable.

Signal /Radio Jamming: A sort of Denial of Service attack that hinders the communication between the nodes by occupying the medium.

Node-capturing/Device-tampering: In this the attacker physically takes over the sensor node and replaces it by their own malicious node. In this the attacker gains full control over the node that is captured and in turn causes harms to the network.

Path-based DoS Attack (PDoS): In path-based DoS attack, the adversary overwhelms the sensory nodes as it floods the multiple hops end-to-end communication path either with replayed packets or injects some spurious packets which overpower sensor nodes from a long distance. Exhaustion in batteries and diminished system availability of nodes are impacts of this physical attack.

Node Outage: This attack is applied logically or physically to the network, outage means loss of connectivity it tends to stop the functionality of the network components. Most of the Node services or operations are stopped because of this attack.

Eavesdropping: It is a type of attack where digital communications are intercepted by a person .It is possible because of the wireless characteristics of RFID system that helps the attacker to take out confidential information such as password or any other data which in turn makes the system vulnerable.

IV. RECOMMENDED SOLUTIONS FOR SECURITY IN IOT

Recommended solutions for security in IoT are examined in three categories

IV.1. SECURITY SOLUTION FOR APPLICATION LAYERS AND SUPPORT LAYER

According to Prof. A. Devipriya in A Novel Survey on Internet of Things Security and its Application, this topic contains two sub-layers. In first sub layer, local applications and related middleware functions are there which should be secured with various techniques. For example, encryption techniques can be used in smart transportation systems, while steganography techniques are used in intelligent home/ intelligent metering systems. The second sub layer resembles national uses and the security systems of their which ensure the security of data sent and received. Hence, various security techniques are applied in these systems based on the extent of each system such as authentication, authorization, access control list, selective disclosure, intrusion detection, firewall, and antivirus.

According to M.U. Farooq in A Critical Analysis on the Security Concerns of Internet of Things (IoT), intruders access is prevented by authentication method is functional in support layer and incorporated individuality identification is in application layer. The security identity method is same as there in network layer. The only difference is they are focusing on authentication with the help of some cooperating services. Hence, the user can choose the information he wants to share with these services. Security of data is one of the issues of these layers. A variety of safety measures are taken on IoT by security system they are:

- Anti-virus software and safe programming testing against service loopholes and hostile code injection.
- Temporary cache development and verification of data against hostile operations
- Session check methods to stop attacks like redo session and hijacking
- Boundary check, resource access control and data encryption methods to keep away from privacy leakage

The IoT weak against many attacks as described previously. Hence, intrusion detection is a critical concept for IoT set up in this world like building automation, smart grids, smart metering and industrial automation. A security mechanism widely called IDS (intrusion detection system) detects attacks against a system during action analysis. Once attack is detected its information is logged or an alarm is reported by IDS. There are many intrusion detection techniques like data mining technique, anomaly detection technique, statistical analysis, etc.

DOI: 10.15680/IJIRCCE.2017. 05032281

IV.2. SECURITY SOLUTION FOR NETWORK LAYER

The security of network layer can be inspected in two main sub-layers that are wireless and wired. The development of protocols for authentication and key management is one of the initial actions in wireless security sub-layer. For example, IP security protocol (IPSec) is developed to secure the network layer and SSL/TLS is developed to secure the link in the transport layer. They provide confidentiality, authenticity and integrity in the each layer. Also by using PPSK (Private Pre-Shared Key) for each device or sensor associated with the network, offers an additional security measure to IoT system. The access domain for each kind of device can be defined easily by providing different unique keys. In addition, disabling of default passwords and guests in the network devices such as routers and gateways should immediately be done after the installation of a new network device. This includes password management, strong password policies and periodic change of passwords.

The wired sub-layer security is concerned about the devices, which communicate with each other using wired medium in the IoT system. Some common security techniques that are applied in wired type of networks are firewalls and Intrusion Prevention System (IPS). If a network has IPS or firewall, it can check network packets intensely that are predestined towards destination. Though, existing IoT system has no ability in terms of packet filtering and packet inspection. There are researches going on this issue where network security researchers are trying to develop a low resource hungry firewall for IoT that gives the capability of packet inspection.

IV.3. SECURITY SOLUTION FOR PERCEPTION LAYER

The perception layer security measures are taken long times back before IoT. Equipment’s such as RFID readers, GPS, gateways, sensors and other devices require to be secured efficiently. In the top 10 IoT vulnerabilities poor physical security has identified by OWASP. First of all we have to ensure that only the authorized people can access the sensitive data produced by devices or physical objects. In order to do that, we need to define the policies for physical identity and access management. In similar manner the process of authorization and the process of authentication and its requirements are to be satisfied by IoT.

Collection of data is an important issue in this layer. There are some recommended security techniques such as encryption multimedia compression, water marking, stenography, intellectual property and time session which can be used for multimedia data collection. For image data collection image compression and Cyclic Redundancy Check can be used to secure images

Cryptographic processing is one among the main tasks in securing the sensor data on IoT. These operations includes encryption and decryption, key and hash generation, and sign and verify hashes that are commonly used in order to guarantee privacy of data.

Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, Sheueling Chang Shantz in Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks (2005) compare two asymmetric algorithms Elliptic Curve Cryptography (ECC) and RSA on sensor nodes and proves that efficiency of ECC greater than RSA, and asymmetric cryptography is applicable to resource-controlled hardware. Therefore, researchers are focusing on reducing the complexity of asymmetric cryptographic algorithms and the key distribution protocols.

These sorts of researches and improvements make cryptographic mechanisms more applicable in the context of wireless sensor network. Although unique customized solutions are created but still there has been no standardized method for implementing the services.

Risk Assessment is a fundamental element of IoT security which finds out the scope of the probable threat and the risks associated with the IoT system. This process output helps in identifying the appropriate controls to reduce or eliminate the risks during risk mitigation process. There are many Guidelines that have been developed by many organizations for conducting risk assessment such as the International Standards Organization (ISO); the U.S. National Institute of Standards and Technology (NIST) and the International Electrotechnical Commission (IEC).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

V. SUMMARY

Layer of IoT architecture	Devices	Threats	Solutions
Application layer	Medical app, enterprise computing, transportation app, mobile app, etc.	social engineering, Loggers/sniffers, injection, DDoS, session hijack, etc.	Authentication, access control list, selective disclosure, IPS, firewall, antivirus, IDS, data verification, session inspection, boundary inspection, data encryption.
Support layer	Information processing, cloud computing, data analysis, data storage, etc.	Data tempering, unauthorized access, Denial of service, etc.	Same as application layer.
Network layer	2G or 3G communication network, internet, broad TV network, mobile network, etc.	Man in middle, wormhole, Selective forwarding, blackhole, Sybil, etc.	TSL/SSL, IPSec, IPS, PPSK, firewall, etc.
Perception layer	RFID reader, gateway, sensor, GPS, etc.	Spoofing, signal jamming, PDoS, node outage, eavesdropping , etc.	Authentication, authorization, cryptography, stegenography, image processing, etc.

Table 1: summary IoT threats and solutions

VI. CONCLUSIONS

IoT is a new and rising technology that has lured a considerable amount of the people attention from all around the world .With the help of some major contributions this technology has been made adaptable into our daily life. However there are some vital issues addressing security concerns of this new technology and they need more effort to be solved properly and make this technology complete. Our analysis of some smart home devices painted a disturbing picture. Despite an almost constant stream of media reports of hacking incidents and cyber attacks, there are still many devices that do not use encrypted communications or proper authentication methods. In this paper .the major security concepts of IoT were reviewed and analyzed extensively. The challenges posed by it and its various requirements were collected and analyzed and were segregated under different headings. All kinds of security threats with respect to the field of IoT that may become a barrier while implementing it or while its development have been discussed and classified with respect to the layers of IoT architecture namely application layer ,support layer, network layer, perception layer. Then finally the various solutions to these problems have been introduced such as firewalls and cryptographic mechanisms and new directions of research have also been discussed.

REFERENCES

[1] OWASP, Internet of Things Project.https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[2] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications , 3, 164-173. https://doi.org/10.4236/jcc.2015.35021

[3] IEC Market Strategy Board (2014) Internet of Things: Wireless Sensor Networks.http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[4] Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internet of Things. Procedia Engineering, 15, 2087-2092. https://doi.org/10.1016/j.proeng.2011.08.390

[5] Cloud Security Alliance (2015) Security Guidance for Early Adopters of the Internet of Things (IoT). https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

[6] Farooq, M.U., Waseem, M., Khairi, A. and Mazhar, S. (2015) A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications , 111, 1-6. https://doi.org/10.5120/19547-1280

[7] Yang, X., Li, Z., Geng, Z. and Zhang, H. (2012) A Multi-Layer Security Model for Internet of Things. Springer International Workshop on Internet of Things , Vol.312, Changsha, 17-19 August 2012, 388-393. https://doi.org/10.1007/978-3-642-32427-7_54

DOI: 10.15680/IJIRCCE.2017. 05032281

[8] Wind River Systems (2015) Security in the Internet of Things.http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
[9] Zolanvari, M. and Jain, R. (2015) IoT Security: A Survey.http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec/index.html
[10] ITU-T. Y.2060: Overview of the Internet of Things.http://www.itu.int/rec/T-REC-Y.2060-201206-I
[11] Sujitha, R., Raghavan, N.V., Suganya, K.S. and Devipriya, A. (2014) A Novel Survey on Internet of Things, Security and Its Application. International Journal of Advanced Information and Communication Technology , 1, 8.
[12] Polk, T. and Turner, S. (2011) Security Challenges for the Internet of Things.http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf
[13] Raza, S. (2013) Lightweight Security Solutions for the Internet of Things. No. 139, Mälardalen University Press Dissertations.http://www.diva-portal.org/smash/get/diva2:619066/FULLTEXT02.pdf
[14] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C. (2005) Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. IEEE International Conference on Pervasive Computing and Communications , Kauai Island, 8-12 March 2005, 324-328. https://doi.org/10.1109/PERCOM.2005.18