International Journal of Engineering & Technology, 7 (4.39) (2018) 109-111

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Study on Internet of Things (IoT) Threats

Vikas Reddy.S [1*], Chandrashekara.S N [2]

[1] *Department of Computer Science & Engineering S J C Institute of Technology, Chickballapur, Karnataka, India*
[2] *Department of Computer Science & Engineering C B Institute of Technology Kolar, Karnataka, India*
**Corresponding author E-mail: vikasreddycs@gmail.com*

Abstract

This paper is mainly related to the threats that are trending on the Internet due to many objects being connected. There are many threats which are discussed in this paper and the main one would be privacy invasion, that is attacking the data by the attackers on the Internet. The solutions would be using authentication keys on both the ends using technologies such as arduino, wireshark, secure databases and secure protocols. The different applications of Internet of Things (IoT) are in health-care management and in our daily activities. Hence we apply security measures so that all the data will be secured and the users can happily interact.

Keywords: *arduino; wireshark*

1. Introduction

IoT is something which is used on daily basis. In the present world IoT is used almost everywhere such as in washing machine, water heater, air conditioning, vehicles etc. Hence IoT is nothing but all these objects interconnected over the Internet. These devices are referred to as objects which are interconnected in a complex manner. The users are also treated as objects wherein they are connected to various objects and can communicate with them. When communicating, all the data is stored or transferred through the Internet. This causes the arise of threats. While communicating, a third person could hack the line and utilize the data. This is usually referred to as privacy threats. There are various layers of the IoT in which different types of attacks can occur. The aim of this paper is to find appropriate solutions for all the threats. This becomes really essential since the IoT is a growing technology which uses other upcoming technology like database system. Hence it is a must that the objects are interconnected without a threat of the data being stolen by an attacker. IoT is hetero in nature and dynamic which makes it difficult for the appropriate solution, but does not make it impossible.

2. Related Works

[1] Threat Implications of the Internet of Things: In this paper authors proposes that there are several objects connected to each other via internet systems which is known as IoT. These objects are the physical representation of data. They are related to each other producing and consuming information. Two objectives are being discussed namely the connectivity of network, the object-embedded information produced and consumed by the entities with or without the user's intervention. The changing environment of these networks causes huge cyber risks. Hence, the attack metric software must be less granular since we are considering dynamic networks. Some of the factors that the relation between the objects are affected by population of entities, which is increasing rapidly due to which complexity and cost also increases and they are being more hetero in nature. The physical distribution of the systems, mobility, heterogeneity causes capture attack of systems as well as information. Cyber attacks may also disrupt and destroy the target and the final type of attack is the manipulation attack where the users are manipulated with their decision cycles. IoT is changing from being a controlled technology to an opportunity based platform but this would not stop the attackers and hence the IoT is developing to become more secure.

[2] Exploring the Threat from Insiders using the Internet-of-Things: In this paper authors say that IoT technology is divided in to 3 layers: hardware, middleware and application. Insider threats happens when members in an organization wrongly use their protected login which cause a wrong encounter on the integrity of the organization's machines.

[3] Smart World of Internet of Things (IoT) and It's Security Concerns: In this paper authors say that IoT is basically a web of embedded devices consisting of sensors, software and have a network that helps them to transfer and receive information which is a mixture of micro electro-mechanical wireless systems, Internet and micro services. IoT can be used at any place, anytime, any context, for anything, any device, for anyone. IoT market gained its growth as first increase in the number of broadband users, secondly the connection cost is minimized by Wi-Fi, sensors. IoT is used in big data and business analytics. Real-time examples of IoT are the smart fridge, smart cities, intelligent shopping system, connected security systems, thermostats, cars, electronic appliances, etc. The challenges faced by this industry are bulk data processing, security, confidentiality, connectivity, high bandwidth and power consumption.

[4] Threat Analysis and Attacks Modeling in Routing Towards IoT: In this paper authors say that operation of routing in IoT system is based on network attributes and autonomous system num bers. Mapping system is required to provide ID for the relevant location when the packet is sent to corresponding ID. Mapping system for the Routing LOCators (RLOC) of the gateway that belongs within the Loc/ID Separation Protocol (LISP) domain is

hosting the destination Endpoint IDentifiers (EID) given in the packet then returns the EID-to-RLOC information and encapsulate the packet towards the obtained RLOC and send it. There are several ideas for the Locator/Identifier split area. The general attacks on IoT devices include spoofed, altered or replayed routing, energy drain attack, data integrity attack, sniffing attack, sinkhole attack, sybil attack, wormhole attack, HELLO flood attack, acknowledgement spoofing, selective forwarding attack, black hole attack, homing attack, node replication attack, etc.

[5] Security Threats in the Application layer in IoT Applications: In this paper authors say that IoT is basically connecting anyone and anything to the Internet. There are three layers namely perception, network and application. Hence security is always needed for all these three applications. The most widely used application layer protocol is MQTT. As IoT is a complex, heterogeneous interconnected system of smart devices many protocols are used at the application layer. According to the devices and the requirements the protocols are chosen and the security at this level is highly important. These protocols basically control the devices present in the network. The application layer being the last layer is useful for guaranteeing the data integrity, data confidentiality and data authenticity. Hyper Text Transfer protocol (HTTP), Constrained Application Protocol (CoAP), web socket, Message Queue Telemetry Transport (MQTT), Advance Message Queuing Protocol (AMQP) are the few application layer protocols. Some of the security threats at application layer are Malicious code injection, Denial-of-Service attack, phishing attack, sniffing attack etc which can be counter measured by authentication, intrusion detection, risk assessment and the encryption methodologies are incorporated for data security. Hence in the future an application layer protocol must be selected just by looking at the device features and network requirements and availability.

[6] Securing the IoT world: issues and perspectives: In this authors say that IoT is found everywhere and used by everyone and thus brings threats such as interoperability, security and privacy. Mainly, we can find a solution in the perception, transportation and application levels of the IoT model. There is a huge risk to the security due to the hetero nature of all the devices and limited resources. Marai malware affecting twitter, PayPal etc are some of the attacks at platforms used by more number of people. The perception level is exposed to physical attacks, Denial of Service attacks, routing attacks, data transit attacks. Security threats at transportation layer are routing attacks, DoS Attacks and at application level are data leakage. Data confidentiality, availability and integrity are some of the security goals. Hence to achieve these goals we make use of secure communication protocols such as IEEE 802.15.4 which could be prone to data transit attacks but can be solved by AES-CCM algorithm which is a standard solution. Hence the main focus is on the communication protocols in order to secure data at IoT.

[7] Cyber Security – IoT: In this authors say that in the current generation, many devices are connected. Some of the top security concerns are device cloning, sensitive data exposure, DoS, unauthorized device access. None of the manufacturers give importance to the security rather give it to the selling price. The security problems are identification of authentic devices and preventing a user to analyze clear text traffic. The system uses technologies such as Wi-Fi, GSM and also exchange keys for authentication, sensors, safe databases to be on the safer side. The software requirements are operating system: Linux, Arduino IDE, programming language: C, Wireshark etc and hardware are Arduino and ultrasonic sensor. Data is encrypted to prevent important data leakage. Hence this model uses less cost but has huge security benefits.

[8] Internet of Things Security-A Review of Risks and Threats to Healthcare Sector: In this paper authors say that the IoT has a concerning risk with data since it has a lot of data on aboard. It deals with reliance on wireless and health care. All the health-care devices have become more smarter, efficient because of being able to use data via internet. These being independent is a huge risk for the data entering into unauthorized hands. Threats are split into two variations, external security and internal security threats which are dangerous in the matter of life of a patient. Cyber security is a efficient method of reducing such risks. The Google Analytics (GA) can be a great method to monitor the device, user's behavior and hence minimize the risk. GA is less expensive. There is an overall increase in the health sector data security incidents from 2013 to 2015. The different security threats in a health-care system could be a mistaken bugs or hamper in the IoT sensor devices connected to patients monitor their pressure, temperature, heart beats etc. and track their activity, behavior. Data backups, authorization etc are some countermeasures to reduce the risk. Hence applying the security in the field of health-care is crucial.

[9] End-to-End Trust and Security for Internet of Things Applications: In this authors say that the IoT is a interconnection of various objects using RFID, sensors, cloud computing etc. The architecture of IoT applications consists of four shades: IoT devices, communications, the cloud, presentations and actions. With this the security and privacy threats are also increasing. They are hetero in nature as well as have limited resources. Attack can happen at device end, at the cloud and also at the communication networks. Hence security must be provided in each of these ends. This is given by representing a 3D secure model which informs where exactly can an attack occur. Some of the security challenges are IoT's open architecture, system limitations, lack of standardization, software vulnerabilities, insufficient trust and integrity. Some solutions such as fog computing can be implemented which removes the gap between the cloud and the internet and also other solutions like implementing security policies such as layering and limiting provides for risk mitigation.

[10] A Taxonomy of IoT - Security and Privacy Threats: In this author says that the technology used in order to control security and solve privacy issues are Design Science Research (DSR) methodology. The main issues could be with the sensors used in IoT technology such as RFID and Wireless Sensor Network (WSN). Objects which are connected to each other on the internet are the susceptible part of the IoT with their less abilities increase the risk of security breaches over networks. Hence the solution would be based on the features of the object which adds a dimension in the security that helps in understanding the privacy issues. The object characteristics dealing with automation, intelligence, storage and processing are related to security dimensions dealing with confidentiality, integrity, availability and access control. Hence this relation is used to minimize the risks. The evaluation process is on the sensors, RFID using the concept of Disney magic band and city of Chicago array of things. Hence this provides maximum security and allows communication through highly secured channels.

Table 1: Overview of algorithms/protocols used

Sl No	Names of Algorithms /Protocols	Quick Look
1	Hash lock agreement	Real tag ID is substituted by pseudo-ID to avoid information disclosure
2	Randomized hash lock agreement	It selects enquiry/answer mechanism considering a random number.
3	David's Digital Library RFID agreement	It uses pirate-random function to implement authentication
4	Distributed RFID enquiry/answer authentication agreement	It is a enquiry/answer two-way authentication agreement.
5	MQTT(Message Queue Telemetry Transport)	This is developed for centralized data collection and analysis of connected smart devices.
6	AMQP(Advance Message Queuing Protocol)	This protocol can do message orientation, queuing. It also supports

		point-to-point, publisher/subscriber models, routing and switching.
7	CoAP(Constrained Application Protocol)	It is expected to use in the constrained environment with constrained resources and constrained network.
8	XMPP(eXtensible Messaging and Presence Protocol)	It is advised to use for real time communication and for streaming XML data between network entities.
9	DDS(Data Distribution Service)	It is used for machine-machine and device-device communication.

3. Conclusion

IoT being hetero can be attacked easily on the Internet. Some of the solutions are using models that make these hetero devices more secure with the data that is being accessed on both the ends. The other solutions such as authentication keys, google analytics, secure database for storing data are used. The better ideology and easier one would be that each device be installed with a local database accessed by only the owner of the device. When transferring the data, it must be securely packed with unused bit and send through a direct link to the other end which would store the data in its own database. This would make it extra secure.

References

[1] Covington, Carskadden (2013). Threat Implications of the Internet of Things. 5th International conference on cyber Conflict.pp.1-5,9-10

[2] Nurse, Erola, Agrafiotis, Goldsmith, Creese, Cyber Security Centre. (2015). Smart Insiders: Exploring the Threat from Insiders using the Internet-of-Things. International Workshop on Secure Internet of Things.

[3] Jonathan Charity, Jian Hua (2016). Smart World of Internet of Things (IoT) and It's Security Concerns. 2016 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data.

[4] Lokulwar, R. Deshmukh (2017) . Threat Analysis and Attacks Modeling in Routing Towards IoT. International conference on I-SMAC .

[5] Swamy, Jadhav, Kulkarni (2017). Security Threats in the Application layer in IOT Applications. International conference on I-SMAC.

[6] Mario FRUSTACI, Pasquale PACE, Gianluca ALOI(2017). Securing the IoT world: issues and perspectives. 2017 IEEE Conference on Standards for Communications and Networking (CSCN).

[7] Swapnil Naik,Vikas Maral. Cyber Security – IoT. 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.

[8] Nasser S. Abouzakhar, Andrew Jones, Olga Angelopoulou (2017). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector.(2017)E International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).

[9] Sulabh Bhattarai and Yong Wang.End-to-End Trust and Security for Internet of Things Applications. EEE COMPUTER SOCIETY.

[10] Badr Alsamani, Husam Lahza. (2018).A Taxonomy of IoT: Security and Privacy Threats .2018 International Conference on Information and Computer Technologies.