International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 12, Number 1 (2019), pp. 113-118

Critical Security Issues on Internet of Things

Gabriela Mogos
College of Computer and Information Sciences
Prince Sultan University, Riyadh, Saudia Arabia.

Nor Shahida Mohd Jamail
College of Computer and Information Sciences
Prince Sultan University, Riyadh, Saudia Arabia.

Abstract

Lots of analysis and development work goes on within the field of internet of Things. Gartner, Inc. has conjointly foretold that 6.4 billion connected things are in use worldwide in 2016 and can reach 20.8 billion by 2020. Internet of Things has such a large amount of applications in today's day to day life like Home automation, Healthcare, Smart grid, sensible automobile etc., and its generating large quantity of data which these devices are sharing. It results in several security issues like the way to secure these devices, knowledge and communication from unauthorized access. IoT uses minimal capability "things" (devices) and wireless technology for communication that makes it a lot of vulnerable. While without providing enough security, the promising benefits of Internet of Things will be misused and worthless. In this paper we are going to discuss in short regarding internet of Things, its applications, security necessities, security problems and major security threats.

Keywords: Internet of Things, Security, Security Design, Software Security

I. INTRODUCTION

The Internet of Things (IoT) paradigm has gained immense quality in recent years. IoT devices are equipped with sensors and/or actuators [1] [2]. IoT devices embrace personal computers, laptops, tablets, good phones, PDAs, good home appliances and alternative hand-held embedded devices [12]. IoT is networking of our day to day devices that don't seem to be solely autonomous in nature however conjointly has sensing capability that permits these devices to understand their surroundings, perceive what's happening and act consequently. Higher call is taken by process the detected knowledge at node, device hub or in cloud. Based mostly upon the processed knowledge these devices will take selections autonomously or might propagate data to users in order that users will take the simplest call [2]. The interconnected device networks will result in an oversized range of intelligent and autonomous applications and services that may bring important personal, skilled, and economic advantages [10], leading to the emergence of a lot of knowledge central businesses. These devices got to share their knowledge to multiple parties like net services, good phone, cloud resource, etc. By creating it accessible through web is that the main goal of IoT therefore a lot of and a lot of objects get joined however it conjointly brings the key considerations to the current technology. One in every of the most considerations that the IoT should address is security and privacy [3] [4]. The foremost vital challenge in convincing users to adopt rising technologies is that the protection of information and privacy. This paper attempt to cowl the safety and privacy aspects associated with web of Things paradigm. We've mentioned concerning numerous applications of IoT and key security problems and security needs in IoT. Key considerations concerning knowledge security, network security and communication security has been conjointly mentioned well.

Finally, we have mentioned concerning many security attacks that may be performed by attackers to misuse the information, devices, and networks. The security of information and network ought to be equipped with these properties like identification, confidentiality, integrity and undeniability. Completely different from internet, the IoT are going to be applied to the crucial areas of financial system, e.g., medical service and health care, and intelligent transportation, therefore security desires within the IoT are going to be higher in convenience and dependableness.

II. SECURE DESIGN

In general, the IoT is divided into four key levels [4].

The foremost basic level is that the sensory activity layer (also referred to as recognition layer), that collects all types of knowledge through physical instrumentality and identifies the physical world, the data includes object properties, status etc; and physical equipment embody RFID reader, all types of sensors, GPS and alternative equipment. The key part during this layer is sensors for capturing and representing the physical world within the digital world.

The second level is network layer. Network layer is liable for the reliable transmission of knowledge from sensory activity layer, initial process of knowledge, classification and chemical change. During this layer the data transmission is relied on many basic networks, that ar the web, mobile communication network, satellite nets, wireless network,

network infrastructure and communication protocols are essential to the data exchange between devices

The third level is support layer. Support layer can establish a reliable support platform for the application layer, on this support platform all reasonably intelligent computing powers are going to be organized through network grid and cloud computing. It plays the role of mixing application layer upward and network layer downward.

The application layer is that the uppermost and terminal level. Application layer provides the personalized services per the requirements of the users. Users will access to the internet of factor through the application layer interface victimization of tv, pc or mobile instrumentality then on.

III. INTERNET OF THINGS APPLICATIONS

Internet of Things has numerous applications in day to day life as delineate in Figure 1 is discussed on IoT applications.

- ***Home automation***: good home or home automation will have numerous options like energy observation, good lights, temperature observation, humidness observation, smoke detector, security and police investigation, smart door, baby observation, good appliances etc. [10].
- ***Healthcare:*** Patient observation, personnel health observation, remote patient observation etc.
- ***Retail:*** Retail sector additionally has numerous applications like observation of inventory and sales in real time.
- ***Industrial:*** provide chain management, logistical management etc.
- ***Transportation:*** Parking management, traffic management, transportation management, vehicle observation and trailing, good cars etc.
- ***Security and Surveillance:*** Home security, building security, atmosphere security.
- ***Good Infrastructure:*** Smart parking, street lightening, Pollution observation, atmosphere observation, waste management, disaster management etc.

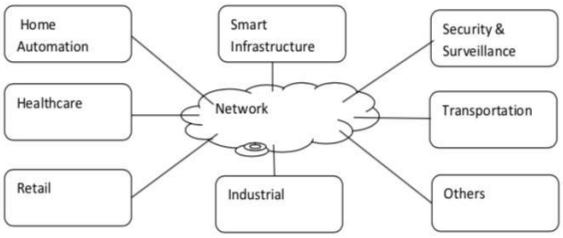

Figure 1. Internet of Things Application

IV. INTERNET OF THINGS SECURITY ISSUES

Wherever networks would be deployed at massive scale security are going to be a significant concern. There are often some ways a system might be attacked by disabling the network availability; pushing corrupt information into the network; accessing personal information; etc. [4]. The 3 physical parts of IoT is RFID, WSN and cloud area unit liable to such attacks [5] [8].

Due to ability among completely different devices and devices with restricted resources, it becomes terribly tough to using the standard security mechanisms directly within the good things [6]. The key security problems with IoT devices area unit as follows:

Table 1. Hardware Issues

Hardware Issues	Description
1. Computational and Energy Constraint	Most of the strongest cryptologic algorithms wants an ample computation and can't be ported simply to devices that are battery driven and uses low-power processor with low clock rate.
2. Memory Constraint	Traditional security algorithms weren't designed consistent with restricted memory area as these devices uses spacious RAM and drive. Whereas IoT devices has restricted memory (RAM and Flash memory) in contrast to the standard devices like computer, Laptop, etc.. These devices use Real Time software package (RTOS) or General-Purpose software package (GPOS) of light-weight version. Therefore, IoT security schemes ought to even be memory economical as standard security algorithms can't be used directly for securing IoT devices.
3. Tamper Resistant Packaging	Many of the IoT devices are deployed remotely that makes these devices a lot of at risk of physical tempering. By device capture assailant will extract secret keys, get access to unauthorized information, modify programs or replace them with malicious nodes. Thus tamper resistant packaging should be wont to shield these devices from attacks [15].

Table 2 Software Issues

Software Issues	Description
1. Embedded Software Constraint	IoT devices use Real Time operative Systems (RTOS), that are embedded with these devices thence these devices have terribly tiny network protocol stack and it ends up in lacking additional security modules [12].
2. Dynamic Security Patch	IoT devices are tiny and mobile in nature and has such a lot of forced. Thus it'd be terribly tough to put in a dynamic security patch as OS or protocol stack may not support updated code and library [16].

Table 3 Network Issues

Network Issues	Description
1. Mobility	Most of the IoT devices are mobile in nature and joins or leaves a proximal network while not configurations. Thus wireless security algorithms is also required.
2. Scalability	As a lot of and a lot of devices are becoming connected with net that raises the problems like quantifiability within the security.
3. Multiplicity Of Devices	IoT network has devices like computer to low finish RFID tags that conjointly raises the considerations like capability of single security theme to handle devices with completely different security problems.
4. Multiplicity Of Communication Medium	IoT devices are connected domestically or globally through web. Thus it's tough to use a security rule which may be operated at each wired and wireless network.
5. Multi-Protocol Networking	Some of the IoT devices may not be mistreatment informatics protocol for host-host communication, whereas most of the IoT devices use informatics protocol. These multi-protocol communications among completely different devices once more creates the matter to use ancient security schemes.
6. Dynamic Network Topology	Mobility nature of IoT devices makes a dynamic topology as these devices may be a part of or leave a network at any time from anyplace. The temporal adding and exiting characteristics of those devices makes it troublesome to use existing security model that doesn't support these styles of fast changes within the topology.

V. INTERNET OF THINGS SECURITY REQUIREMENTS

In the IoT, multiple sensors, little laptop chips and communications devices are going to be integrated with physical objects like appliances to change communication between them and different computing devices like cloud servers, computers, laptops and smartphones. These devices can exchange immense quantity of information with every other. Thus knowledge security is extremely vital considerations for IoT. There are many factors that must be taken care whereas making a security resolution for the IoT devices [5]. The protection necessities that are expected to be met by the IoT security schemes are discuss below.

Table 4. Data Security Necessities

Data Security Necessities	Description
1. Data Integrity	Whereas exchanging the information if some attackers modifies the contents of information then it will be brought immense injury to our system. Therefore, knowledge integrity whereas communication is extremely a lot of vital.
2. Data Confidentiality	Confidentiality should be preserved whereas communication. No matter knowledge IoT devices can share ought to be encrypted mistreatment sensible cryptography rule thus assailant won't be able to interpret the particular knowledge. Thus IoT devices ought to be tack together in such a way in order that they can share knowledge to solely approved device.
3. Data Availability	Principle of availableness says that knowledge ought to be obtainable forever to authorized IoT devices and users.

Table 5 Access Level Security Requirements

Access Level Security Requirements	Description
1. Authentication	Authentication is employed to envision weather a human action device is legitimate or not means that if device A has sent some knowledge to B then authentication mechanism is employed to make sure that it's come back from A. it's conjointly wont to verify that a certified user has access to IoT device.
2. Access Control	Access management is employed to confirm that Associate in Nursing echo or authorized IoT devices solely have access to those things that these devices are authorized for.
3. Availability	Principal of convenience states that information or IoT devices ought to be perpetually out there to licensed parties.
4. Non-Repudiation	Not- repudiation doesn't permits a human activity party to refute the claim of not causation the information that it's sends.

VI. TYPE OF ATTACKS ON INTERNET OF THINGS

There will be numerous sort attacks risk on the IoT. Attacks on privacy and authentication of IoT devices and knowledge. These attacks will be of various sorts like active attacks during which attackers attacks the devices and knowledge by compromising it and may results in immense harm. There will be passive attacks like intercepting the information that is extremely tough to find [8]. The assailant performs numerous activities like electronic jamming the network, message sniffing, device compromising, etc [11]. For gaining unauthorised access to knowledge or devices thus IoT services will be build dysfunctional. Following are the attacks which might be utilized by attackers to hamper the IoT services.

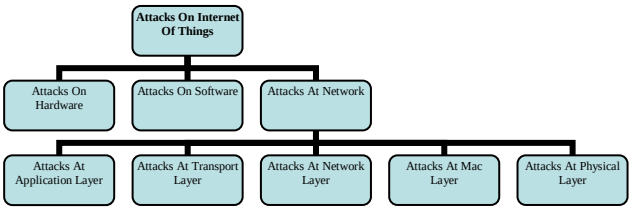

Figure 2. Type of Attacks on Internet Of Things

Attacks on Hardware

Attackers will compromise the hardware by meddling with information, keys, ASCII text file. This sort of attacks will be solely attainable if attackers get physical access to the IoT devices. Hardware attacks will be solely prevented if these devices have some tamper resistant style.

Attacks on Software

IoT devices are embedded with software and system code [12]. These devices store non-public knowledge and secret info like cryptologic keys that ought to be secure at any value. Code attacks are often performed by finding the vulnerabilities within the software or system code running on the IoT devices. These kinds of attacks primarily take devices within the exhaustion state by offensive the code resources. Code compromise ends up in threats like loss of crypto keys, keep knowledge, OS failure, buffer overflow etc. [7]. Code compromise is often done victimization attacks like replay, fabrication, interruption, denial of service attacks etc.

Attacks on The Network

An assailant will perform many attacks on the IoT network at completely different layers of the protocol stack [9]. However, attacks are frenzied at completely different layers are mentioned below.

Table 6. Attacks On The Network

Attacks on The Network	Description
1. Attacks at Application Layer	At the applying layer numerous attacks like SQL injection, application hijacking, and fraud are often performed. Through these attacks attackers not solely gain access to non-public knowledge however they conjointly compromise full application code or programs.
2. Attacks at Transport Layer	Transport layer provides method to method communication and flow management between processes. At transport layer denial of service (DOS) attacks like flooding is incredibly common that is finished to deliberate congestion of communication channels through causing unneeded traffic [14] [17]. Asynchrony attack will be conjointly performed at transport layer by making pretend messages and asking to correct the error to alternative process [17]. This ends up in loss of energy and unneeded participating finish points in finishing up spoofed directions.

3. Attacks at Network Layer	At network layer attacks like scientific discipline packet spoofing are often tired that attackers send incorrect supply address. Once receiver gets this packet it will replies back to the present incorrect address. This will end up in state of affairs within which wrongdoers can intercept the message or attacker is performing arts DOS attack [14]. Selective forwarding attacks compromise the node and build it send the info to choose nodes rather than all [13]. Flooding attacks causes high traffic in channels by making state of affairs like congestion within the network by causing useless messages in terribly high range.
4. Attacks at Mac Layer	At MAC layer level node to node digital communication takes place. Raincoat layer conjointly ensures error management at node to node level. Attacks like collision may be performed at this level by transmittal packets at the same time on the shared channel that causes to corruption of knowledge. Receiver starts discarding the corrupt packets once it detects the error and evoke retransmission to sender and will generate congestion scenario between 2 endpoints. Battery exhaustion attacks essentially cause's high traffic during a channel and makes its accessibility very restricted to the nodes. Such disruption within the channel is caused by sizable amount of requests and transmissions over the channel.
5. Attacks at Physical Layer	The Physical layer of an IoT will modulation and reception, choice and generation of carrier frequency, encoding and secret writing, transmission and reception of information. ECM attacks will be performed at physical layer by occupying communication medium between IoT devices therefore these devices won't be able to communicate with one another. Another common attack which may be done at physical layer is device meddling to urge the access of sensitive information [9] [15].

VII. CONCLUSION

In the recent years IoT has attracted several analysers to hold out research during this field. Applications and implementation of this domain is increasing at a good rate, because it has been expected that around twenty billion devices are going to be connected by 2020. As most of the IoT devices are helpful in our day to day life thus while not providing enough security and privacy folks won't use this technology. During this paper we've surveyed all security flaws that exist or could exist within the IoT which will be terribly prejudices within the implementing and development of secure IoT infrastructure. It'll facilitate the investigator to pay additional attention in those explicit space that is additional at risk of attacks. Higher and appropriate cryptanalytic algorithms consistent with hardware, code and network, constraints may be developed, which can make sure the secure communication among the devices and its users. Intrusion detection techniques may be enforced to create secure and sturdy IoT infrastructure.

REFERENCES

[1] Zhou, Q., & Zhang, J.: Research prospect of Internet of Things geography, Geoinformatics, 19th International Conference on (pp. 1-5). IEEE (2011).

[2] Yu, Y., Wang, J., & Zhou, G.: The exploration in the education of professionals in applied Internet of Things Engineering, Distance Learning and Education (ICDLE), 4th International Conference on (pp. 74-77). IEEE (2010).

[3] Jing, Qi., et al.: Security of the internet of things: Perspectives and challenges, Wireless Networks 20.8 (2014): 2481-2501.

[4] Weber, H. Rolf.: Internet of Things–New security and privacy challenges, Computer Law & Security Review 26.1 (2010): 23-30.

[5] Stankovic, J. A.: Research directions for the internet of thing, Internet of Things Journal, IEEE, 2014, 1(1), 3-9.

[6] Desai, P., Sheth, A., & Anantharam, P.: Semantic gateway as a service architecture for IoT interoperability, Mobile Services (MS), 2015 IEEE International Conference on (pp. 313-319). IEEE

[7] Xu, S. X., & Chen, J. Z.: Analysis of buffer overflow exploits and prevention strategies, Applied Mechanics and Materials 2014, (Vol. 513, pp. 1701-1704).

[8] Perrig, A., Stankovic, J., & Wagner, D.: Security in wireless sensor networks. Communications of the ACM, 47(6), 53-57(2004).

[9] Sastry, A. S., Sulthana, S., & Vagdevi, S.: Security threats in wireless sensor networks in each layer, International Journal of Advanced Networking and Applications, 4(4), 1657 (2013).

[10] Atzori, L., Iera, A., & Morabito, G..: The internet of things: A survey, Computer networks, 54(15), 2787-2805(2010).

[11] Xu, W., Trappe, W., Zhang, Y., & Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (pp. 46-57). ACM (2005).

[12] Kocher, P., Lee, R., McGraw, G., Raghunathan, A., & Moderator-Ravi, S.: Security as a new dimension in embedded system design, Proceedings of the 41st annual Design Automation Conference (pp. 753-760). ACM (2004).

[13] Wood, A. D., Fang, L., Stankovic, J. A., & He, T.: SIGF: a family of configurable, secure routing protocols for wireless sensor networks, Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (pp. 35-48). ACM (2006).

[14] Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M.: Denial-of-Service detection in 6LoWPAN based Internet of Things. In 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 600-607). IEEE (2013).

[15] Ravi, S., Raghunathan, A., & Chakradhar, S.: Tamper resistance mechanisms for secure embedded systems. In VLSI Design, 2004. Proceedings. 17th International Conference on (pp. 605-611). IEEE.

[16] Deng, J., Han, R., & Mishra, S.: Secure code distribution in dynamically programmable wireless sensor networks. In Proceedings of the 5th international conference on Information processing in sensor networks (pp. 292-300). ACM (2006).

[17] Maróti, M., Kusy, B., Simon, G., & Lédeczi, Á.: The flooding time synchronization protocol. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 39-49). ACM (2004).