Security Challenges Facing IoT Layers and its Protective Measures

Tariq Aziz Rao
Department of Computer Science
Virtual University of Pakistan
Lahore, Pakistan

Ehsan-ul-Haq
Department of Computer Science
Virtual University of Pakistan
Lahore, Pakistan

ABSTRACT
The Internet of Things (IoT) is profoundly affecting people's routine lives in various fields ranging from petite wearable devices to enormous commercial systems and it has been predicted that in upcoming few years, more than 50 billion devices will become the part of the IoT as many of these applications have already been developed. However, the maintenance of security and privacy is a great challenge that restricts the broad implementation of IoT. As the Internet of Things has no standardized architecture, so various types of attacks occurred on different layers of IoT. Some proficient security methods have already developed to protect the IoT system but not enough, so, there is a dire need to do more. This paper describe the security challenges facing four basic layers of IoT and suggest the protective measures to enhance the reliability and robustness of the IoT. Also, portrays the comparative analysis of security challenges between IoT and traditional network.

Keywords
Internet of things, security, privacy, layer architecture, security challenges, protective measures

1. INTRODUCTION
In general phraseology, the Internet of Things (IoT) is referred to a new world where all the devices and appliances are linked with each other via the internet and people can utilize them collectively to perform some complex task efficiently. It is not a solitary technology rather it is a collection of several technologies that work together in a proper cycle. Several devices have been developed which are being utilized as IoT, such as, Laser Scanner, Radio Frequency Identification Devices (RFID), Infrared Sensor, Global Positioning System (GPS), etc. It has been predicted that in 2020, more than 20.4 billion devices will become the part of the Internet.

Internet of Things got its control over our routine life with the RFID and wireless connectivity. Today, IoT is extensively practical to social life appliances like smart home, transportation, smart grid, security, education, fitness, healthcare, environmental monitoring, etc.

IoT security and privacy protection are of utmost importance because IoT devices are more likely and easier to be attacked by malevolent persons to fulfill their wicked desires. In 2016, a DNS service provider Dyn faced a severe Distributed Denial of Service (DDoS) attack, which caused an interruption in service of various popular websites like Amazon, Facebook and Twitter [1]. User security should be ensured by thwarting unauthorized access because once an IoT layer is compromised, hackers could easily get the access through a compromised node. Furthermore, virus, malicious software, and hackers might disturb the information and data integrity as a result of which the information anxiety will openly threat the whole IoT environment.

Security domain of Internet of Things is interesting and vivid. If looks from a security point of view, many loopholes find in architecture of IoT. In most IoT structure, Wireless Sensor Network and IP based Wireless Sensor Network are vulnerable and security risk. If any node is compromised, the malicious users can get the information and cause a serious destruction of the entire system.

IoT devices are mostly installed at geographically discrete locations, so, there exists a wireless communication amongst them. In the wireless network, exploitation of vulnerabilities can lead to DoS attack [2], which is a very grave challenge in IoT atmosphere. In practical applications like emergency quick response system and traffic monitoring, the data collection must be quick and precise. No delay can be acceptable in the IoT environment because the delay in response can cause a denial of service (DoS), so, the data transmission for IoT atmosphere is very essential.

Section 2 portrays the basic four layers architecture of IoT. Section 3 describes the security challenges facing different IoT layers with examples of various types of attacks on these layers. Protective measures required to be taken in IoT layers are discussed in Section 4. Section 5 explains the comparative analysis of security challenges between traditional and IoT network. In Section 6, finally, present the conclusion of this research.

2. FOUR LAYERS ARCHITECTURE OF IOT
In recent past, several architectures of IoT have been proposed because no single agreement has come forward. The basic architecture of IoT is consisting of four layers, such as Perception Layer, Network Layer, Processing Layer and Application Layer as shown in Figure 1. A brief introduction of these four layers architecture of IoT is as under: -

2.1 Perception Layer
This layer consist of various sensors such as infra-red, RFID, QR code and ZigBee for gathering information about the surroundings like humidity, temperature, pH level pressure, force, etc.

2.2 Network Layer
This layer consist of physical components and network communication software which are responsible for transmitting information acquired from the sensors of the perception layer to other layers without any intervention.

2.3 Processing Layer

This layer is also called middleware layer that analyzes, stores and processes an enormous amount of information. This layer provides miscellaneous services to the lower layers and also capable to automatically compute and process information. Many technologies like cloud computing and big data processing employ in processing layer.

2.4 Application Layer

This layer provides the services to the user as per his requirement. Typical applications of IoT are smart home, smart cities, smart transportation, healthcare, utilities etc.

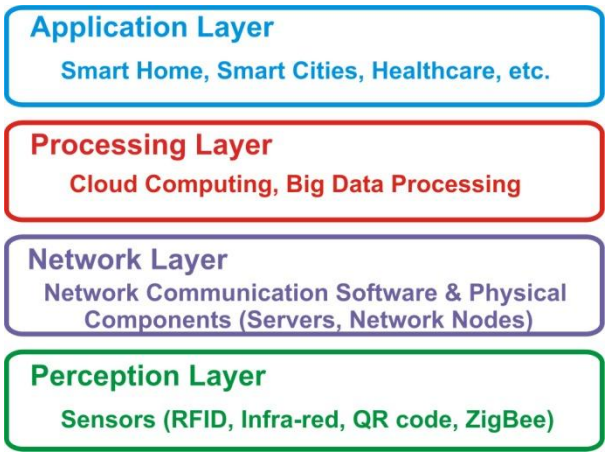

Fig 1: Four Layers Architecture of IoT

3. SECURITY CHALLENGES IN IOT LAYERS

Due to the high acceptance rate of IoT, the number of devices connected to the internet increasing day by day. Various security challenges facing IoT layers, some of which are discussed as under: -

3.1 Security Challenges in the Perception Layer

In perception layer, hardware attacks are most general attacks. This layer includes various kinds of sensors such as, RFID, ZigBee, WSN which are located at one place for a long time may be physically attacked. Various IoT devices such as smart wearable devices, video games are collecting information about us and this information may be shared or accessed by some hackers for illegal motives. General attacks on perception layer are described below: -

3.1.1 Forged node insertion

In forged node insertion attack, the attacker can insert a false or malevolent node between the actual nodes of the network to get the access and control on the data stream of the network for his nefarious design. The attacker can also stop the transmission of actual data or destroy the entire IoT environment.

3.1.2 Malevolent code insertion

The attacker can insert the malevolent code to get the access to the network and cause the unavailability of network services.

3.1.3 Hardware Jamming

Attacker can damage the node by replacing the original parts of its hardware. The attacker can obtain the information regarding communication key, cryptographic key, routing table, etc. by capturing the gateway node or changing the electronic integration which is a serious security threat.

3.1.4 Slumber denial attack

In IoT network, nodes on the distant places are mostly powered by the replaceable batteries, so, these nodes are programmed to slumber when these are not in use due to the saving of battery life. Attacker remain the node awake and stop them to snooze by feeding false input to the node which results in power expenditure, so, the node power failure.

3.1.5 Wireless Sensor Network node jamming

Attacker can create the denial of service of the IoT by jamming the signals of Wireless Sensor Network or sending noise signals over the network.

3.1.6 Noise in Data

There is a high probability that the data may contain incomplete or false information because the transmission of data has occurred over the wireless network in which nodes are located at large distance from one another, so, the distortion of data can be very risky in this scenario.

3.2 Security Challenges in the Network Layer

Authentication and reliability of data that is being transported in the network layer is the primary security challenge. Some security challenges to network layer are:-

3.2.1 Denial-of-Service (DoS) attack

In DoS attack, servers or devices are unable to provide the services to the user. Transfer of data between devices and their sources are shut down due to DoS attack.

3.2.2 Sinkhole attack

This attack canceled the data security and drops all the packets instead of delivering these packets to its destination properly because of attacker through all signals from wireless sensor network nodes to an unchanged point which is very harmful in IoT environment.

3.2.3 Man-in-Middle attack

In this attack, the attacker does not need to actually appear on the location of a network, he just uses the communication protocol of IoT to interfere the two sensor nodes to get the classified information.

3.2.4 RFID authorized access

Tags are reachable to anyone because there is no safe authentication system in RFID systems. This means that tags can be influenced easily [3].

3.2.5 Gateway attack

Connection between the sensors and the internet infrastructure is cut off in this attack. This attack also includes DoS attack or routing attack in which false or no information is transmitted from internet to nodes/sensor.

3.2.6 RFID Spoofing

In RFID spoofing attack, attacker targets the RFID signal to get the information stamped on RFID tag. Hacker uses this type of attack to transmit his own data using original id [4] and can obtain the full access to IoT system.

3.3 Security Challenges in the Processing Layer

In this phase, data is sent to the cloud, so the cloud attack is one of the most vulnerable assaults in this layer. Some possible attacks on this layer are:

3.3.1 Application security

Mostly applications on cloud Software as a Service (SAAS) are delivered through web services, so the attacker can easily utilize the web to get the access to IoT network and embezzle the information to fulfill his evil desires. Various security issues on SAAS had identified by Open Web Application Security Project [5].

3.3.2 Primary infrastructure security

Developers always try to develop an application safe but its security remains in danger due to lower layers of IoT which is also the responsibility of service provider.

3.3.3 Data security in cloud computing

Data backup provided by the service provider is a major security concern. Data processed and stored on a cloud as plain text, so, the SaaS providers have the responsibility to ensure the security of data, so that, no malicious user can access the classified information.

3.3.4 A Threat to shared resources

Shared resources are also a security threat because the attacker can observe all the shared resources between the virtual machines and get the requisite information for his illegitimate motives.

3.3.5 An Attack on Virtual Machines

Security of Virtual Machines (VM) is of utmost importance and any security breach can cause the failure of entire IoT environment.

3.3.6 Third-party relationship

Platform as a Service (PaaS) provides a third party web service component i.e. mashups [6] and when more than one source is combined in mashups, it increases the security risk.

3.4 Security Challenges in the Application Layer

The application can be compromised as well as shutdown effortlessly due to security issues. The malevolent attack can reason of virus in the application program code that activates the application to break down. Sometimes, applications are abortive to bring authenticated services for which they are planned to accomplish or provide the service inaccurately. Some general threats to this layer are given below: -

3.4.1 Malevolent code attacks

This type of attack could be malicious "worm" which is capable of attacking Internet-enabled devices like security cameras and home routers [7]. This type of attack could break Wi-Fi of a car and get control over steering wheel which results in a serious accident.

3.4.2 Software defenselessness

Non-standard codes written by the programmers can be increased the software vulnerabilities. The malicious users to fulfill their immoral desires use this method.

3.4.3 Phishing attacks

Attacker can be accessed the classified information through infect email or website from spoofing the user's confirmation identity.

3.4.4 Virus, Spyware, and Worms

Attacker can infect the system with malicious software which results in pilfering information, denial of service or corrupt data.

4. PROTECTIVE MEASURES TAKEN TO SAFEGUARD THE IOT LAYERS

In order to eliminate the chance of malicious attack by hackers or reduce to the lowest level, the following protective measures should be observed to safeguard the basic four layers of IoT: -

4.1 Protective measures for Perception Layer

Following protective measures should be observed to safeguard the perception layer from malicious attacks: -

4.1.1 Authentication of Devices

Authentication of the devices should be ensured before getting into the network in order to keep away the malicious devices from IoT environment, so that, forged data follow in the network could be prevented.

4.1.2 Secure Physical designing of end devices

Perception layer's attack can be resolved by secure physical designing of end devices. The components of devices such as radio frequency circuit, chip selection, etc. must be of high quality. For example, good design of antenna for wireless communication could be able to communicate over a long distance.

4.1.3 Safe Booting

To check the integrity and authentication of the software on different devices of IoT network, cryptographic hash algorithm can be utilized. In fact, most of the hash algorithms cannot be implemented on end devices of the network because these devices possess very low computing power; therefore, WH and NH cryptographic algorithms are the optimum solutions of this problem [8].

4.1.4 The Integrity of data

To decrease the risk of data tempering, each device utilized in the IoT environment should be provided error detection system such as checksum, a parity bit, etc. The cryptographic hash function should be used to make the more secure IoT network [9].

4.1.5 Anonymity

Attacker can hide classified information such as identity, location, etc. by injecting node in the IoT network. K-anonymity approach is the best solution to this problem [10] as it works better on low processing devices.

4.2 Protective measures for Network Layer

Below mentioned precautionary measures should be considered to protect the network layer from hackers' attack: -

4.2.1 Confidentiality of data

Data confidentiality can be ensured by preventing illegitimate access of the nodes of the IoT network. Point to point encryption can be utilized for authentication purpose. In this process, classified data is immediately converted into cipher code which is unbreakable.

4.2.2 The Integrity of data

Integrity of data can be ensured by using the cryptographic hash function on the data which ensured that it is not tempered on reaching receiving side. Furthermore, by

applying error correction mechanism, mitigation difficulty can also be resolved.

4.2.3 Secure Routing

Secure routing is the played a vital role in safe usage of sensor systems as most of the routing conventions are not stable, so, routing security can be ensured by routing the data through several paths that increase the error exposure of the network.

4.2.4 Spoofing

GPS location system can be faced the spoofing attack. For this problem, no perfect solution is provided as yet, however, S. Daneshmand et al [11] described the GPS system techniques, which is best.

4.2.5 Inside and outside attacks

Attack from inside the network can be secured by security conscious ad-hoc routing modus operandi and attack from outside the system can be secured by encryption and authentication, so that, the hacker cannot join the IoT network.

4.3 Protective measures for Processing Layer

Following countermeasures should be practical to defend the processing layer from any malevolent attack: -

4.3.1 Encryption to secure classified information

The basic purpose of encryption is to secure the sensitive data, so, usually data is stored or sent to the cloud is in encrypted form to avoid any security breach. Today, various type of encryption methods are being used which are helpful in defeating side channel attack and secure the IoT environment.

4.3.2 Data Fragmentation redundancy scattering

In data fragmentation redundancy scattering, the classified data on the cloud is splitting into various fragments and stored on various servers [12], therefore, the risk of data escape is minimized as a fragment of the data do not have any important information.

4.3.3 Hyper safe lockdown

Hyper safe lockdown and guard the write protected memory pages from being customized. Furthermore, pointing index is constrained that change the data into the pointer indexes [13].

4.3.4 Web firewall applications

Web firewall applications can identify a possible attacker, so such applications should be used to protect the IoT environment.

4.4 Protective measures for Application Layer

The following security measures should be adopted to protect the application layer from any nasty attack: -

4.4.1 User validation

Integrity and encryption mechanisms are vital for the security and privacy of a system because any security breach can be caused by any data stealing and unauthorized access to the IoT environment.

4.4.2 Special policies and permissions

Special policies and permissions should be observed for accessing and controlling the IoT structure. Outgoing/incoming traffic and the access request of the system can be permitted or restricted by access control lists.

4.4.3 Use of Anti-virus, anti-adware and Anti-spyware

All these software are crucial to ensure the security, consistency, confidentiality, and reliability of the IoT environment.

4.4.4 Use of Firewalls

Authentication password and encryption method can be break due to a weak password, therefore, firewalls should be used which monitor the incoming and outgoing network traffic.

4.4.5 Risk Assessment techniques

Risk assessment techniques detect threats of the IoT system, so, the application layer should be secured by the risk assessment. For this purpose, update the firmware of the system devices in order to strengthen the security measures.

5. COMPARATIVE ANALYSIS OF SECURITY CHALLENGES BETWEEN TRADITIONAL NETWORK AND IOT

Security concerns in the Internet of Things (IoT) layers and its countermeasures are discussed at length in above two sections. This section describes the difference in security challenges facing IoT and traditional network, which are given as under: -

5.1 Resources

Usually, the traditional network comprising upon a personal computer, servers and smart-phone whose resources are adequate, whereas, IoT system is composed of FRID and WSN nodes whose resources are inadequate. So in order to maximize the security in a traditional network with less usage of computational power, user can utilize the combination of lightweight and complex algorithms. However, in IoT to maintain the equilibrium between security and computational power, only lightweight algorithms can be utilized.

5.2 Communication ways

Wireless media is used for connection between the nodes of IoT, which result in a security breach. In the internet, mostly communication made through a more secure wire or wireless communications, which is faster as well. Wireless connections are built on top of complex secure protocols in mobile internet, whereas, it is nearly impossible to employ in IoT nodes due to limited resources.

5.3 Risk Factor

Risk factor is greater in IoT system as compared to traditional network because a large number of IoT applications are being used in routine life and in case of lose control over these systems, it may be created a great security risk. On the other side in a traditional network, if users do not provide their classified information themselves, then there is no way to attack any malicious person to get their secret information for his criminal motives.

5.4 Data Formats

Even though different devices in the internet but with the abstraction of the operating system like Windows or UNIX, their data formats are almost the same, whereas, there is no operating system in IoT, just a simple embedded program for the chip [14]. Due to different nodes in IoT environment, there comes various chip hardware that results in diverse data formats.

6. CONCLUSION

Like other revolutionary technologies, IoT has got popularity in every lifestyle and attention of researchers from the last few years. However, it also faces various security and privacy issues. This paper articulates the four basic layers architecture of IoT and different types of attacks on these layers with instances. Protective measures to safeguard these layers are also suggested to prevent and secure the IoT system from the security terrorization. A comparative analysis of security challenges between a traditional network and IoT environment is made and came on the conclusion that IoT system facing a lot of security challenges due to limited resources, elevated risk factors, and heterogeneous data formats.

Therefore, in order to strengthen the security measures in IoT network, new lightweight cryptographic algorithms and key management schemes are required to implement which take the lowest computational power. Furthermore, there is a dire need to shift every IoT device with an updated kernel/firmware and should include the capability to frequently update as new threats are originated. This paper will prove supportive for the researchers as well as IoT applications' developers from a security perspective. However, the production of most dominant operating systems for IoT is still a great challenge for developers to maximize the trust of people on IoT network.

7. REFERENCES

[1] Ren, Z., Liu X. and Ye R. 2017. Security and Privacy on Internet of Things. In 7th IEEE International Conference on Electronic Information and Emergency Communication (ICEIEC), pp. 140-142.

[2] Adat, V. and Gupta, B. B. June, 2017. Security in Internet of Things: issues, challenges, taxonomy, and architecture, Telecommunication Systems, pp. 1-19.

[3] Uttarkar, R. and Kulkarni, R. 2014. Internet of Things: Architecture and Security. International Journal of Computer Application, 3(4), pp. 12-19.

[4] Ahmed, M. M., Shah, M.A. and Wahid, A. 2017. IoT Security: A Layered Approach for Attacks & Defenses. in IEEE International Conference on Communication Technologies (ComTech), pp. 104-110.

[5] Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z. and Bloodsworth, P.C, 2014. Semantic security against web application attacks. Information Sciences, vol. 254, pp. 19-38.

[6] Hashizume, K., Rosado, D. G., Fernandez-Medina, E. and Fernandez, E. B. December, 2013. An analysis of security issues for cloud computing. Journal of Internet Services and Applications, pp. 1-13.

[7] Kumar, S. A., Vealey, T. and Srivastava, H. 2016. Security in Internet of Things: Challenges, Solutions and Future Directions. 49th Hawaii International Conference on System Sciences (HICSS), pp. 5772-5781.

[8] Avoine, G., Bingol, M. A., Carpent, X. and Yalcin, S. B. O. October, 2013. Privacy-Friendly Authentication in RFID Systems: On Sublinear Protocols Based on Symmetric-Key Cryptography. IEEE Transactions on Mobile Computing, 12(10) pp. 2037-2049.

[9] Alizadeh, M., Salleh, M., Zamani, M., Shayan, J. and Karamizadeh, S. 2012. Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID. Recent Researches in Communications and Computing, pp. 45-50.

[10] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A. and Kikiras, P. 2015. On the Security and Privacy of Internet of Things Architectures and Systems. IEEE International Workshop on Secure Internet of Things (SIoT), pp. 49-57.

[11] Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A. and Lachapelle, G. 2012. A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array. ION GNSS12 Conference, pp. 1–11.

[12] Singh, Y., Kandah, F. and Zhang, W. 2011. A secured cost-effective multi-cloud storage in cloud computing. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 619–624.

[13] Kumar, S., Singh, S. P., Singh, A. K. and Ali, J. June, 2013. Virtualization, The Great Thing and Issues in Cloud Computing. International Journal of Current Engineering and Technology, pp. 338–341.

[14] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J. and Qiu, D. November, 2014. Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20(8), pp. 2481-2501.