Layers of IoT Architecture, its Security, Challenges and Protective Measures

Mehjabee Zeba[1*]
Department of Computer Science and Engineering
New Delhi, India

DR.Jawed Ahmed[2]
Department of Computer Science and Engineering
New Delhi, India

Abstract- Internet of Things is something which is highly affecting people's daily lives in different areas of world which ranges from small wearable devices to broad commercial systems. The implementation of IoT is controlled by the privacy and security which is a big challenge. Some types of attacks occurred on IoT layers, because there is no standardized architecture of IoT. There are a number of expert methods to secure the system of IoT, but these methods are very few so we have to do more. This paper consists of security challenges and the protective measures in four layers of IoT, which helps to increase the strength and reliability of IoT. It compares IoT over traditional network security challenges.

Keywords - Internet of things, IoT Layer Architecture, Security challenges, Protective Measures, Comparative Analysis.

I. INTRODUCTION

The Internet of Things (IoT) is a number of different connected devices, people, objects and services that may be communicate with each other and also share data and information in order to obtain a common goal in various field. It also hold a number of applications, including transport, agriculture, healthcare, energy production and distribution. [1]

It is also referred as a modern world where every systems and devices are connected with each other through internet. It has a group of various technologies that works together in a proper way. A number of devices being utilized as IoT have been developed for example, Laser, Infrared Sensor, Radio Frequency Identification Devices (RFID), Scanner, Global Positioning System (GPS), etc. [2]

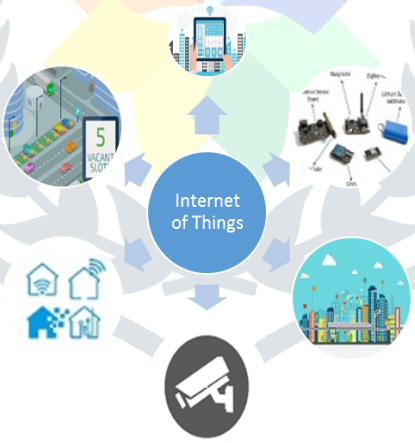

Fig 1: Internet of Things

Through the RFID and wireless connectivity the IoT acquire its control over everyone routine life. Now a day, some applications of IoT such as the transportation, smart home, smart grid education, security, fitness, environmental monitoring, healthcare etc. which are extensively practical to social life.

The privacy and security of IoT are most important because IoT devices can easily attacked by any attacker to achieve their illegal desires. User security must be secure through the preventing of illegal access because if an IoT layer is compromised, then a compromised node could be accessed by the attacker. Virus, hackers and malware may interrupt information and data integrity, resulting in a threat to information for the entire IoT environment. Within most of the IoT structure, IP - based Wireless Sensor Network and Wireless Sensor faces the security risk. The attacker can cause a serious demolition of whole network after getting the information.

Within the IoT device there is wireless communication because IoT devices are installed in the geographically separate locations .Exploitation of danger can conduct to DoS attack in wireless network, [3]. It is a great challenge in IoT atmosphere. In practical applications data collection must be quick such as quick response system traffic monitoring and emergency. Due to delay in response, denial of service (DoS) may be occur in the IoT environment, so no delay could be acceptable, the data transmission is very essential for IoT atmosphere.

II. FOUR LAYER ARCHITECTURE OF IOT

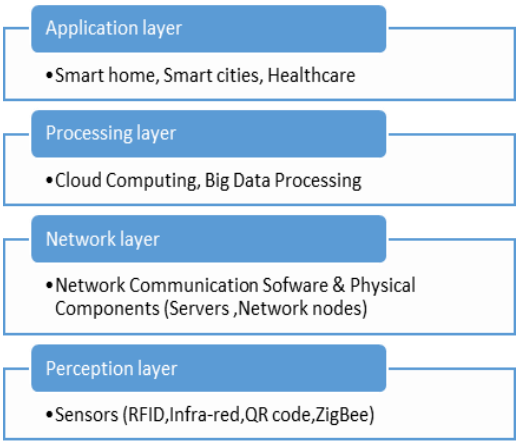

Fig 2: Four layer architecture of IoT

In recent year, not a single agreement has come in. So several architectures of IoT have been proposed.The IoT architecture contains four layers, these are Perception Layer, Network Layer, Processing Layer and Application Layer, illustrated in Figure 2.

1. The Perception Layer
The perception layer made up of numerous sensors which helps in collecting information about the surroundings such as pressure, force, humidity, temperature, pH level etc. for example infra-red, RFID, QR code and ZigBee.

2. The Network Layer
In network layer, it is the responsibility of the network communication software and physical components to transfer information by perception layer sensors to other layers without participations.
.
3. The Processing Layer
Enormous amount of information is analysed, stored and processed in this layer. It is also called middleware layer. This layer is capable to automatically compute and process information and also provides miscellaneous services to the lower layers. Many technologies employ in processing layer, like cloud computing and big data processing.

4. The Application Layer
This layers supply the services as required by the user. The smart cities, smart transportation, smart home, healthcare, utilities etc. are the typical applications of IoT.

III. LITERATURE REVIEW

A lot of research has been done in security in IoT. We focus on security and protective measures on different layers of IoT in this section.
Mian Muhammad, Ahemd Munam, Ali Shah, Abdul Wahid has explained the working of layers of iot and security loopholes were discussed. To prevent the iot network countermeasures were adopted and also to overcome the deployment issues and make it more secure some improvements were suggested.
Tariq Aziz Rao and Ehsan-ul-Haq has described the layers of iot. To enhance the reliability and robustness protective measures were suggest. Between iot and traditional network comparative analysis of security challenges were done.

IV. SECURITY CHALLENGES ON LAYERS OF IOT

A number of internet - connected devices will be growing every day because of the high IoT acceptability rate Different kind of security challenges faced by layers of IoT, Some of them will be considered below:-

A. Perception Layer Security Challenges of IoT

Most general attacks in perception layer is hardware attacks. A number of sensors like WSN and RFID, ZigBee, are present which may get physically attacked if it is detect at same location for a long time. The smart wearable devices, video games are the IoT devices which has information to us and this types of information can be share or access by attackers for illegal purpose.

(i) The Forged Node Insertion
Such an attack, False or malevolent node can be inserted by the hacker between actual nodes of network. The attacker may also destroy the entire IoT environment or stop the transmission of actual data.

(ii) Hardware Jamming
The hacker destroys the node in this way through the changing of the actual hardware components. The hacker obtains information about cryptographic key, communication key, and routing table by changing the electronic integration or seizing gateway node, etc.

(iii) Wireless Sensor Network Node Jamming
Hacker may generate some obstruction to IoT service by jamming Wireless Sensor Network's signals or transmitting noise signals across the network.

B. Network Layer Security Challenges of IoT
The primary security challenge is the authentication and reliability of data. Network layer has few security challenges and they are:-

(i) Denial-of-Service (DoS) Attack
In the case of DoS attack, data transfer between devices and their sources will be shut down. Thus, devices or servers can not able to supply the services to user.

(ii) Man-in-Middle Attack
The hacker interferes with the use of the IoT communication protocol between the two sensor nodes to obtain the classified information, so the attacker could not really need to show up.

(iii) RFID Authorized Access
As tags can be accessed by everyone, RFID systems do not have a safe authentication system. Tags can be easily influenced. [5]

C. Processing Layer Security Challenges of IoT
At this stage, the most vulnerable assaults in this layer is the cloud attack as data can be transmitted on cloud, several feasible attacks are:-

(i) Application's Security
Most of the applications have been delivered by web services on cloud Software as a Service (SAAS), to access the IoT network the attacker can utilize the web very easily and to fulfil his evil desires he embezzle the information [6].

(ii) Cloud Computing Data Security
Data backup is a major security issue for the service provider. Data will be processed and stored as plain text in the cloud, so the responsibility of SaaS providers is to ensure data security, so classified information cannot be accessed by malicious users.

(iii) Attacks on Virtual Machines
Virtual machine (VM) security is most important because a single security breach may cause the entire IoT environment to fail.

D. Application Layer Security Challenges of IoT
Because of security issues, the applications may be compromise and also shut down effortlessly in this layer. There are few threats in this layer as shown below:-

(i) Malevolent Code Attacks
It might be a harmful "worm" that can be attacks on security cameras and home routers which is Internet - enabled devices [7].It can be break a car's WiFi as well as gain control over the steering wheel, leading to a serious accident.

(ii) Phishing Attacks
By spoofing the user's confirmation identity by infecting email or website the attacker can access the classified information.

(iii) Harmful Worms, Viruses, and Spywares
The system will be infected through the malicious software resulting in the information being stolen, (DoS), and data corruption.

V. SOME PROTECTIVE MEASURES PROVIDE THE SECURITY ON IOT LAYERS

Some protective measures could be observed to cancel the possibility of harmful attack through an attacker to decrease the lowest level:-

A. Perception Layer's Protective Measures

Various protective counter measures, the perception layer must be protect against harmful attacks:-

(i) Authentication of Devices

Before entering in network, the devices must be authenticated, so the data that has been forged, follow in the network could be prevented by keeping away the malicious devices from IoT environment.

(ii) Secure physical Design of End Devices

Through the secure physical design of end devices, the perception layer attacks could be resolve. The radio frequency circuit, chip selection, etc. are the components of devices must be of high quality.

(iii) Safe Booting

Cryptographic hash algorithm might be utilized to test the software's integrity and authentication on various IoT network device.

(iv) The Integrity of data

To make the IoT network more secure, use the cryptographic hash function. Data tempering can also be resolved by using error detection system which is checksum, parity bit etc.

B. Network Layer's Protective Measures

Preventive measures must be considered below to secure the network layer by the hacker attacks: -

(i) Confidentiality of Data

For authentication purposes the point to point encryption have been utilized. It must be prevented through the illegal access on the IoT network nodes. The classified data will be immediately converted into non - breakable cipher code in this process.

(ii) The Integrity of Data

The cryptographic hash function can ensure the integrity of data, which ensures that on reaching receiving side it is not tempered. Mitigation difficulty can also be resolved by using error correction mechanism.

(iii) Secure Routing

Secure routing plays an important role in the safe use of sensor systems to stabilize routing conventions. To ensure routing security, the data can routed across multiple paths that increase network error exposure.

(iv) Spoofing

Spoofing attack could be faced with the GPS location system. Still there is no perfect solution to this problem, but S. Daneshmand et al [8] have represented the best GPS system techniques.

C. Processing Layer's Protective Measures

Some security measures to preserve the processing layer against any illegal attack must be empirical:

(i) Encryption to Secure Classified Information

The sensitive data is secured by encryption. There are so many different methods of encryption that can be help to defeat side channel attack and provide the security of the IoT environment as well.

(ii) Data Fragmentation Redundancy Scattering

In the redundancy scattering of data fragmentation, the categorized cloud data can be break into a number of fragments and will be stored on different servers [9].

(iii) Hyper Safe Lockdown

Through this the write protected memory pageswill be protected by customization. So the risk of data disappearing have been minimized there is no significant information on a fragment of the data [10].

(iv) Web Firewall Applications
Web firewall application could be identifies the attacker easily. Therefore, this type of application must be utilized to secure IoT environment.

D. Application Layer's Protective Measures
To secure the application layer against illegal attack, some security measures must be acquired: -

(i) User Validation
For the security of a system encryption and integrity mechanisms are essential because any data stealing and illegal access can cause security breach.

(ii) Special Policies and Permissions
Some particular policies and permissions have been made to access or control IoT structure. The lists of access controls allow or limit incoming / outgoing traffic and system access requests.

(iii) Anti-virus, Anti-adware and Antispyware
The Anti-virus, anti-adware and Antispyware are some software which can be used to ensure the IoT environment's security, confidentiality and reliability.

(iv) Firewalls
Firewalls are used to detect the incoming and outgoing network traffic. Due to the weak password, the authentication password and encryption method can be broken.

(v) Risk Assessment Techniques
Threats might be detected through the risk assessment techniques, thus the risk assessment techniques could be used to secure the application layer. The firmware device system will be updated to enhance security countermeasures.

VI. SECURITY AND PRIVACY FRAMEWORK REQUIREMENT

1. Light Weight and symmetric solutions:- It is used to support resource constrained devices

2. Light weight key management system:- It establishes trust relationship and distribution of encryption material which is done by minimum communication and processing resource

3. Cryptographic techniques:- It prevents the information to be accessible to third parties.

4. Other technique for privacy:- Data identification, authentication and anonymity.

5. Decentralized computing and key management

6. Privacy of personal information

VII. SECURITY CHALLENGES IN TRADITIONAL NETWORK VERSUS IOT

1. Resources
Traditional network resources are adequate as the traditional network consists of personal computers, servers and Smartphones, while IoT system resources are inadequate as the IoT system consists of FRID and WSN nodes. User can use the lightweight and complex algorithms in a traditional network to maximize the security not so much usage of computational power but, in IoT only lightweight algorithms can be utilized, to manage the equilibrium between security and computational power.

2. Communication Ways
For connection between the nodes of IoT the Wireless media is used, due to result in security violation. It is mostly faster to communicate with a more secure wire or wireless communication via the internet. Wireless Internet connections are built in addition to complex secure mobile protocols. Because of limited resources, it is almost impossible to use IoT nodes.

3. Risk Factor
In IoT system, compared to traditional network risk factor is higher because of huge amount of IoT applications will be used in daily life, a great security risk can be created in the event of loss of control over these systems. Whereas in the traditional network there is no way of attacking anyone and obtaining their secret information, unless users themselves provide their classified information.

4. Data Formats

Operating system abstraction such as Windows and UNIX, its data formats nearly the same. A simple program is embedded for the chip, there is no operating system in IoT [11]

. Because of the various nodes in the environment of IoT, different chip hardware resulting in different data formats.

COMPARISON TABLE

LAYERS	ATTACK NAME	EFFECT	COUNTERMEASURES	LAUNCH
PERCEPTION LAYER	The Forged Node Insertion	Fake Data Manipulation	Secure Physical Design	2011
	Hardware Jamming	Data leakage (Keys, routing tables, etc)	Secure Booting	2013
	Wireless Sensor Network Node Jamming	Jam Node Communication	IPSec Security channel	2010
NETWORK LAYER	Denial-of-Service (DoS) Attack	Resource Destruction	Access Control Lists	2010
	Man-in-Middle Attack	Data Privacy Violation	Point-to-Point Encryption	2011
	RFID Authorized Access	Node data can be modified (Read, Write & Delete)	Network Authentication	2014
Processing Layer	Application's Security	Privacy Violation	Web Application Scanner	2014
	Cloud Computing Data Security	Data leakage (User data on cloud)	Homomorphic Encryption	2012
	Attacks on Virtual Machines	Resources destruction	Hyper Safe	2012
Application Layer Security	Phishing Attacks	Data Leakage (User credentials data)	Biometrics Authentication	2017
	Malevolent Code Attacks	Data leakage	Anti-virus, Anti-adware	2012
	Harmful Worms, Viruses, and Spywares	Resource Destruction & Hijacking	Protective Software	2012

VIII. CONCLUSION

In past few years, IoT has been approved in all lifestyles as well as researcher's attention. It has also facing a number of security or privacy issues, though. This paper represents the four fundamental IoT layers architecture and different kinds of attacks in layers of IoT .Some Protective countermeasures are also available to protect the IoT layers. It suggests securing and preventing the security threat to IoT system. The security challenges with the traditional network and IoT are also analysed comparatively. This comparison helps to understand that IoT system faces a huge number of security issues and challenges because of the limited resources, heterogeneous data formats, and elevated risk factors.

It must be requires new lightweight cryptographic algorithms and key management schemes that take the lowest computational power to strengthen security measures in the network of IoT. As new threats arise, every IoT device with an updated firmware needs to be shifted and should also be able to update on a regular basis.

From a security perspective this paper will be helpful for the researchers and also for the IoT application's developers. To enhance people's trust in the IoT network, the development of dominant IoT operating systems remains a major challenge for developers.

IX. REFERENCES

[1] T. Y. F. A. I. Z. Rwan Mahmoud, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures," *The 10th International Conference for Internet Technology and Secured Transactions* , 2015.

[2] E.-u.-H. Tariq Aziz Rao, "Security Challenges Facing IoT Layers and its Protective Measures," *International Journal of Computer Applications* , vol. 179, 2018.

[3] V. a. G. B. B. Adat, "Security in Internet of Things: issues, challenges, taxonomy, and architecture, Telecommunication Systems," pp. 1-19, JUNE 2017.

[4] R. a. K. R. Uttarkar, "Internet of Things: Architecture and Security.," *International Journal of Computer Application,* , pp. 12-19, 2014.

[5] A. L. K. A. H. F. H. A. A. Z. a. B. Razzaq, "Semantic security against," *web application attacks. Information Sciences,* vol. 254, 2014.

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

[7] M. S. M. Z. M. S. J. a. K. S. Alizadeh, "Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID.," *Recent Researches in Communications and Computing,,* pp. 45-50, 2012.

[8] S. J.-J. A. B. A. a. L. G. Daneshmand, "A Low-Complexity GPS AntiSpoofing Method Using a Multi-Antenna Arra," *ION GNSS12* , p. 1–11. , .2012.

[9] Y. K. F. a. Z. W. Singh, "A secured cost-effective multi-cloud storage in cloud computing.," *Conference on Computer Communications Workshops (INFOCOM WKSHPS),* 619–624. .

[10] S. S. S. P. S. A. K. a. A. J. Kumar, "Virtualization, The Great Thing and Issues in Cloud Computing.," *International Journal of Current Engineering and Technology,* p. . 338–341, 2013.

[11] Q. V. A. V. W. J. L. J. a. Q. D. N. Jing, "Security of the Internet of Things: Perspectives and challenges.," *Wireless Networks, 20(8),* , pp. 2481-2501., 2014.