2nd International Conference on Scientific and Academic Research

March 14-16, 2023 : Konya, Turkey

All Sciences Proceedings
http://as-proceeding.com/

© 2023 Published by All Sciences Proceedings

Layered Architecture of Internet of Things-A Review

Muhammad Awais*, Jawaid Iqbal [2]

[1]Software Engineering Department, Capital University of Science and Technology Islamabad, Pakistan
[2]Computer Science Department, Capital University of Science and Technology Islamabad, Pakistan

*(mawaiskhan1808@gmail.com) Email of the corresponding author

Abstract – Nowadays internet of thing is need of every person as it makes life easy and comfortable its object work with sensors and actuator without involving human. This device gets users personal information and store it in internet cloud etc. IoT device has limited storage, power consumption and the capacity of network. Attacker can easily attack and get user information and use its wrong way in this scenario to maintain and keep secure privacy in IoT devices is also big issues so IoT has major issue of security. Its need to identify security threats and attacks and purpose solution to prevent from those attacks. So that every person can use every IoT devices without any kind of fear and hesitation about their privacy and trust and fear of loss private data. In this paper we focus on the layered architecture of IoT with its threat and attack also highlight the suitable solution of each layer's attack and focus on the security goal which used and must achieve in every IoT devices to secure that devices from any kind of attacks and threats that can breach the end user vulnerability and get access of end user's system. We also discuss some useful and existing techniques with services to prevent from different kind of attack that used worldwide.

Keywords – IoT, Security, Privacy, Authentication, Threats, Vulnerability

I. Introduction

Internet of Things(IoT) is a network that help devices to communicate with each other and share data. With the help of sensors and actuator it makes things smart and automatic. Sensors sense and get data from its environment and pass to the actuator that take corresponding action on the basis of predefine rules and regulations. IoT make human life easy comfortable and efficient and by using IoT devices people reduce their effort and make their life easier. IoT devices connected with internet without internet IoT is nothing. Internet work as a backbone in IoT devices. So there are some security and privacy issues that a user can faced during the use of IoT devices.

It is important to protect user security by limiting unauthorized identification and access. By privacy, we mean that the user has sole control over his or her personal information. Reliability is a problem that develops because of the growing reliance on data and IoT-based devices. When we talk about gadget reliability, we imply that they must always function flawlessly and effectively as intended [1]. Through internet any malicious activity can perform that could be dangerous for original user. Attacker can get sensitive information of original user through internet connection and use it an illegal way. Due to these security issues people have some kind of fear and hesitation to use IoT devices. That 'why security is major issues that many user face.

The main challenges in an IoT context are security related issues such privacy, authorization, verification, access control, system setup, information storage, and management (Jing et al., 2014). IoT applications, such as those for smartphones and embedded devices, for instance, contribute to the development of a digital environment for global connectivity that makes life easier by being sensitive to, adaptable to, and responding to, human requirements. Security is not assured, though. When user signals are cut off or intercepted, users' privacy may be violated and their personal data may be exposed.

This issue needs to be resolved in order to provide users confidence regarding their privacy and control over their personal information before the IoT is widely used. Addressing security issues is crucial for the growth of the Internet of Things. In addition to proposing potential ideas for enhancing the IoT security architecture, this study seeks to serve as a valuable guidebook of current security risks and vulnerabilities of the varied IoT environment [2].

II. LITERATURE REVIEW

The term "Internet of Things" refers to a network made up of "smart objects," which are multiple physical objects, sensors, and edge devices that communicate via various Internet resources and are used for a variety of purposes in a variety of industries, including apparel, logistics, health care, and transportation (IoT). It is among the most significant technological revolutions of our time [4].

It is a predecessor to the smart world because it uses pervasive computing and networking to simplify and provide other services, like the simple monitoring of many environmental phenomena. With the development of computing and communication technologies, the quality of the environment and ordinary items, often known as things, objects, or machines, is increasing. Although an IoT architecture may offer a range of solutions for different industries, its major objective is to create a working, scalable, flexible, maintainable, and affordable IoT ecosystem [5].

However, because of their limited resources and the intrinsic IoT environment conditions—basically, the dynamic element, the heterogeneity, and the open and wireless means of communication—connected objects are typically vulnerable. The majority of conventional security mechanisms created so far for the Internet do not meet IoT security needs, making IoT network security a persistently open and difficult problem [6]. Systems are susceptible to hacker exploitation because of the IoT devices' extensive accessibility and interconnectedness. Finding a cutting-edge security architecture that addresses problems with data security, data confidentiality, and data integrity is therefore necessary [7].

In order to secure the IoT, there are still unresolved problems and difficulties that must be overcome. 37 As a result, the IoT systems have security flaws and are open to several attacks [8]. The underlying cause of these defects or successful assaults is that the controls or the underlining architecture are not strong enough to safeguard Internet of Things (IoT)based applications [9]. Security measures should be taken into account for the entire design because each layer of the IoT architecture has distinct security challenges and interacts with other layers [10].

Several different goods and technologies are used at every layer, from sensing to the application. At the edge nodes, these include several sensors and actuators. There are numerous communication protocols, including Bluetooth, Wi-Fi, IEEE 802.15.4, Insteon, dash7, and cellular networks. All of these requirements must be met by a handshake mechanism. In addition, multiple communication technologies, such as ZigBee, 6LOWPAN, wireless HART, Z-Wave, ISA100, Bluetooth, NFC, RFID, etc., are employed at different levels in the same IoT application [11].

With the help of cutting-edge technologies like Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSNs), which are sensed by the sensor devices and then processed for decision-making, on the basis of which an automated action is performed, the fundamental goal of the Internet of Things is to enable autonomous exchange of useful information between invisibly embedded different uniquely identifiable real world devices around us [12].

Due to security issues and challenges every source of internet can exploit and breach the vulnerability. As each architecture layer have some security problems. In this paper we described the IoT elements that purposed different researchers in IoT devices. We also highlight security goals that must achieve to get authenticity, trust and privacy. We have reviewed on each architecture layer of IoT and suitable techniques and solution to resolve that issues and improved layered architecture of IoT which have mac layer and data and assets security layer that is called seventh layer architecture of IoT.

III. Materials and Method

We reviewed the security goals IoT elements, different layered architecture of IoT and related threats that create problem and issue for end users.

A. Security Goals of IoT

In the following section we presented the security goals that help to make IoT devices secure and trustable.

Confidentiality

Confidentiality ensure that information is available just for authorized and authentic user and keep all information private from unauthorized access and information only share with trusted user it ensure that information cannot be disclose and not share with illegal user.

Availability

It is property that ensure availability for authentic user 24/7. Authorize user can get access at any time when user needs. It protects information from DoS and DDoS attack because due to DoS Attack Information is unavailable for authorized user.

Integrity

It is property that ensure information is in its original form and cannot modify by unauthorized user or attack. It performs some techniques and method to keep secure information from attacker. It ensures that information is not disclose.

B. IoT Elements

IoT devices consist of six elements that help to devices work automatically by observing its environment and take action according to pre-defined rules.

Identification

Identification is important part of everything same in IoT it has identification which consists two main parts one is name that get from id and second is address. Each object has different and unique address. By using Electron Product Code(EPC), IPv6 and ubiquitous code we can provide address.

Sensing

Sensing is processing of gathering data from its related environment and after processing get information and send to the database or cloud. There are some sensing devices like FRID, actuator, and wearable sensing devices.

Communication

It is main element of IoT that help devices to send and receive data, files and communicate with each other. For example, NFC, Bluetooth, and Wi-Fi.

Computation

It works like brain of IoT. It controls and manage the computation power of IoT. Like Lite OS.

Services

Four type of services provides for customer.

- Identity related services
- Information Aggregation
- Collaboration Aware services
- Ubiquitous Services

Semantic

It has ability to extract information using resource and decide to send response to device. Like OWL, and RDF.

C. Layered Architectures of Internet of Things

With the help of these layered architecture we can understand easily what kind of threats and attack perform on each layer and what is the suitable solution for that attack to keep secure our network environment.

1. Three Layered Architectures and Security Issues

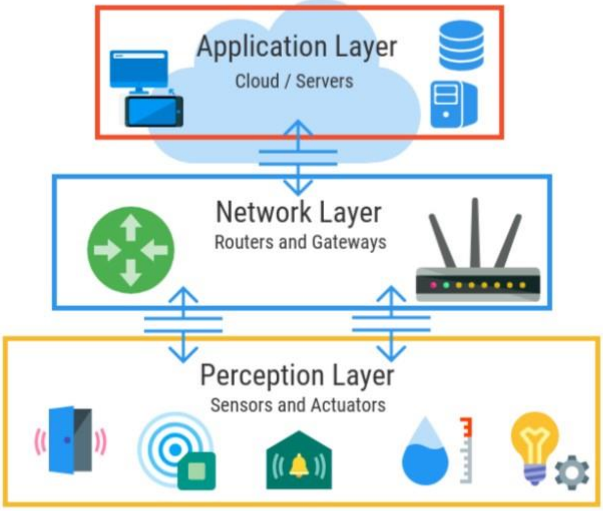

Figure 1. Three-layers IoT [8]

Perception Layer

Perception layer work like human senses. It identifies and sense different kind of things from its environment and collect data from them and after processing it pass information to the network layer.

Security Threats

Eavesdropping attack: It is real time attack that get access to listen private communication that transmitted between sender and receiver over the network and get sensitive information.

Node capture: It is one of most dangerous attack in perception layer. Attacker capture full node of network and get important and key information of sender and receiver that store in particular node.

Malicious Node: In this attacker add malicious node on network to stop the sharing real information and have bad impact on network energy that can destroy the network.

Noise in Data: Due to the fact that data must be transmitted via wireless networks that reach long distances, there is a great likelihood that the data will contain noise, or worse, erroneous or incomplete information. When so much depends on the accurate transmission of data, misleading the data might be dangerous [1].

Timing Attack: In this attack attacker get information about computation times so that attacker get cryptographic keys and know about the password of user.

Network Layer

This layer act like a bridge between perception layer and application layer. It gets information from perception layer and send it to application layer using different kind of protocol. Its basic purpose to transmit information.

Security Threats

Denial of service: It is kind of attack in which attacker create a traffic on particular network to create difficulty for authentic user on that network. So that original user does not get access easily on network.

Men in the Middle: In this attack there is an attacker between sender and receiver communication and get control their communication and can easily modify.

Storage Attack: It is kind of attack in which attacker can get information by attacking on user’s storage devices like cloud. It can change user’s information into fake and incorrect detail.

Exploit attack: Attacker purpose to get fully access on targeted system and get all information from targeted system so that attacker uses it according his needs.

Application Layer

Application layer is defining that how system is interact with user. All IoT apps and IoT-deployed applications are categorized under the application layer. Smart homes, smart cities, smart health, animal tracking, and more applications for IoT are possible. It is accountable for giving the applications the services. Because services are dependent on the data gathered by sensors, they may differ for each application [3].

Security Threats

Cross site scripting: It is kind of attack in which attacker injected wrong script and get completely access on that application, make changes in application and use the original information in wrong way.

Malicious Code: In this attacker injected a part of malicious code that create unexpected impact and issues that may damage the system.

Unauthorized access data: Attacker attack and gain access on whole network then use it data illegal way.

2. *Four Layered Architectures and Security Issues*

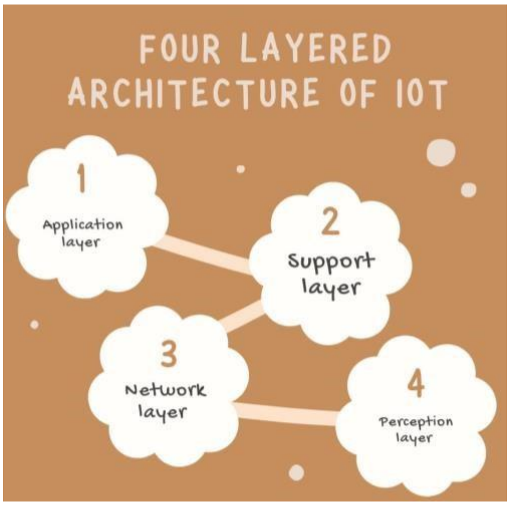

Figure 2. Four-layers IoT

Support Layer

Support layer in four-layer architecture play an important role to achieve security and make strong security level because in three layer there is no security checker information directly send to application layer but in this support layer performs authentication process and protect information from risks and attacks so that only authentic user can send information.

Security Threats

DoS: It is kind of attack in which attacker create a traffic on particular network to create difficulty for authentic user on that network. So that original user does not get access easily on network.

Insider Attack: Attacker is from in organization like employee who use his legal access for illegal intention to gain benefit for his self and misuse of actual information.

3. Five Layered Architectures and Security Issues

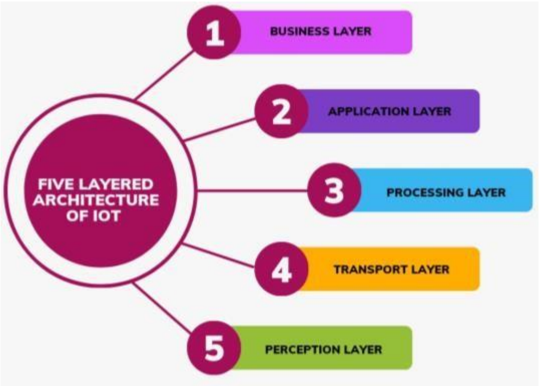

Figure 3. Five-layers IoT

Processing layer or Middleware layer

Processing layer work on big data processing. It eliminates extra information and contain useful information. It solves big data problem because due to big data performance of IoT affect badly.

Security Threats

Exhaustion: when attacker perform dos attack exhaustion occurs and create a traffic on processor of system and damage the processing power of system due to this data is unavailable for original user. It also dangerous for memory sources and battery.

Malwares: Malware is attack in which attacker intention to damage the victim’s system or computer and network. The virus can be injected in any form like script, code, adware, advertising and usb.

Business Layer

Basic purpose of business layer to control application and manage the process of change, creation, and stored information and manage the user’s privacy. Security Threats

Business logic attack: It is kind of attack in which attacker get benefits from websites scripts and poor program algorithm It injected wrong code in database and control information that transmitted between client and database.

Zero-Day-Attack: Attacker create a problem before anyone know about that and attacker has more chances to success in launching this attack. And it’s difficult to identify this attack because there is no detection software at that time attacker's intention to damage vulnerability of system.

Solution of Perception Layer's attacks

By using different kind of firewall, virtual private Network, updated antivirus software, use of HTTPs and SFTP prevent from different attack that occurs on perception layer and avoid to use HTTP and FTP protocol, Public Wi-Fi network. Try to use that firewall which detect and prevent environment and tell the status on regular basis if any kind of malicious activity perform it alert us by showing status good or bad. By using different encrypted method and algorithm can prevent from attacks and transmit save communication.

Solution for Network Layer's attacks

By using Hash Function that can achieve integrity, deploy firewall that detect and prevent any kind of traffic occurs on network during communication and generate a kind of alarm to alert authentic user, monitor and control network devices on daily basis so that prevent from DoS attacks, use patch management techniques that patch security holes in system from where malicious activity can perform and use strong password on storage devices like cloud. By using all these methods prevent from attacks on network layer.

Solution for Application Layer's attacks

By using protocol that provide Authentication, Authorization, and Accountability(AAA), configure and monitor application setting regularly, attaches only trustable devices because sometime malicious code can be perform through USB and spread in system, must have some back up to recover data that loss due to malicious or unauthorized activity, must perform threat assessment and measure application security on daily basis, manage privileges and use intruder detection system prevent from attacks that occur on Network layer.

Solution for Support Layer's attacks

We should manage the network security regularly, use malware prevention software, configure of security, by managing user privileges and by controlling removable devices.

Solution for Processing Layer's attacks

By using anti-spyware software, different kind file and e-mail security method so that any kind of malicious e-mail and attaches file and sources go to spam without disturbing system, updated security algorithm and method that detect malware and take action against that and implement security algorithm that monitor and control any kind of suspicious activity.

Solution for Business Layer's attacks

By hiring trained and educated user who know how to detect risk and threat and manage that risk, apply a proper strategy to monitor system and model for the security purpose.

Improved Architecture of IoT Layered

Improved layered architecture of IoT consist Mac layer that provide authentication and data and assets security layer that make devices secure.

MAC Layer

Each node on a network needs an addressing mechanism and channel access in order to connect with other nodes on that network or others. This is the fundamental purpose of MAC. The main goal of the MAC protocol is to prevent collisions and make it easier for network devices to transport data packets. It is in charge of multiplexing and flow management for the transmission medium. It regulates the data packets' distant shared channels transmission. It provides authentication, error detection code

Data and Assets security layer

It provides protection sensitive data and assets that entered in network it also helps to protect storage from viruses and threats and protect data transformation. It provides protection by checking verification of strong password and authenticate user.

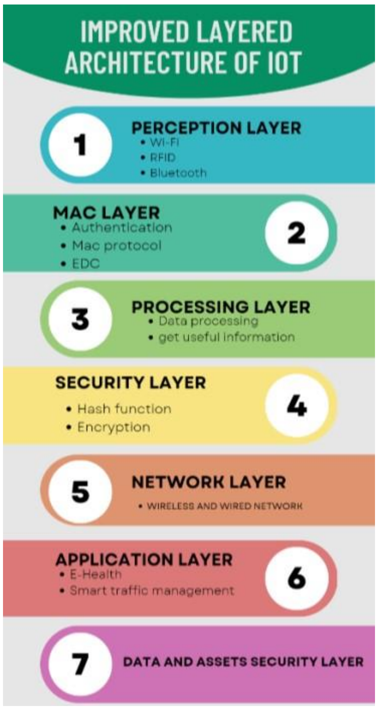

Figure 4. Improved layer architecture of IoT

IV. RESULTS

We discussed the different kind of techniques and protocol and that reviewed services related security, privacy and authenticity.

Table 1. Techniques and Services

No	Techniques	Services
1	Encryption	Confidentiality
2	Hash Function	Integrity
3	MAC	Authenticity
4	Digital Signature	Integrity, Non-Repudiation, and Authenticity
5	Kerberos	Authentication

V. DISCUSSION

We reviewed this pervasive computing environment where sensors and actuators will be connected to both living and non-living "things" and will all be a part of the Internet, in addition to computers and smartphones. IoT security issues and related technologies play a significant part in its implementation. The purpose of IoT security, IoT components, and a security-based study of IoT architecture have all been covered in this paper. We have discussed and examined the security threats related to key IoT technologies and the architecture's security [13].

In architecture first we discuss three layered architecture utilizes wired or wireless methods to carry and/or transmit the data gathered by the sensors. Additionally, it is in charge of establishing connections between the various networks, "smart," and network devices. As a result, it has numerous security problems with information integrity and authentication.

Then the purpose of fourth layered architecture that is security in the IoT architecture is the justification for adding a fourth layer. In a three layer architecture, data is routed straight to the network layer. Sending data straight to the network layer increases the likelihood of encountering attacks. But in four layered architectures there is some security issues then five layered architectures are discussed which have two extra layer business and processing layer. We purposed seventh layered architecture that help to secure data before any malicious action perform and secure that data in storage devices and mac layer provide authentication and help to achieve main IoT security goals.

VI. CONCLUSION

Due to security issues and challenges every source of internet can exploit and breach the vulnerability. As each architecture layer have some security problems. In this paper we highlight the IoT elements that must have in IoT devices. We also mentioned security goals that must achieve to get authenticity, trust and privacy. We have reviewed on each architecture layer of IoT and purposed suitable techniques and solution to resolve that issues and reviewed improved layered architecture of IoT which have mac layer and data and assets security layer that is called seventh layer architecture of IoT.

ACKNOWLEDGMENT

Thankfully, we are aware of our parents' affection for us. Last but not least, we would like to thank our family and friends whose prayers made it possible for us to finish this project.

REFERENCES

[1] Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

[2] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.

[3] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, *18*(9), 2796.

[4] Gupta, S., Gabrani, G., & Arya, P. K. (2022). Intrusion Detection System with Layered Approach to Internet of Things—A Business Paradigm. In *Internet of Things* (pp. 117-132). Springer, Singapore.

[5] Punia, A., Tiwari, M., & Verma, S. S. (2023). The IoT in Security Architecture, Challenges, and Solutions. In *International Conference on Optical and Wireless Technologies* (pp. 405-416). Springer, Singapore.

[6] Swessi, D., & Idoudi, H. (2022). A survey on internet-ofthings security: threats and emerging countermeasures. *Wireless Personal Communications*, *124*(2), 1557-1592.

[7] Ali, A., Mateen, A., Hanan, A., & Amin, F. (2022). Advanced Security Framework for Internet of Things (IoT). *Technologies*, *10*(3), 60.

[8] Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Kashif Bashir, A. (2022). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, *33*(6), e3935.

[9] Aryavalli, S. N. G., & Kumar, H. (2023). Top 12 layerwise security challenges and a secure architectural solution for Internet of Things. *Computers and Electrical Engineering*, *105*, 108487.

[10] Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157.

[11] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721-82743.

[12] Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International journal of computer applications*, *113*(1), 1-7.

[13] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423441.