ISSN: 0975-833X

Available online at http://www.journalcra.com

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

International Journal of Current Research
Vol. 13, Issue, 05, pp.17614-17618, May, 2021

DOI: https://doi.org/10.24941/ijcr.41538.05.2021

RESEARCH ARTICLE **OPEN ACCESS**

SECURITY ISSUES AND THEIR REMEDIES IN INTERNET OF THINGS (IOT)

***Deepak Jyoti**

Assistant Professor, PG Deptt. of Computer Sc. &IT Shanti Devi Arya Mahila College, Dinanagar

ARTICLE INFO

Article History:
Received 20th February, 2021
Received in revised form
25th March, 2021
Accepted 18th April, 2021
Published online 30th May, 2021

Key Words:

IOT, Sensor,
Networks,
Smart objects,
Security.

ABSTRACT

Background: People are using internet anywhere and anytime. IOT is the field which connect people with the devices, which allow people to communicate with connected devices at anytime and anywhere. It has facilitate our life style very deeply. It is very innovative invented technology which facilitate every user to control all connected devices remotely automatically. It facilitates various services to the user at various platforms and applications. Internet of things (IOT) constitutes one of the most important technological development in the last decade in which all smart and heterogeneous devices are connected. These devices are able to communicate to each other through internet. but various challenges are there in such a innovative technology. Security is the big challenge with this technology. If the security leaks then there will be big harm to the sensitive information of the user. The traditional security management mechanisms are not able to apply on IOT because of heterogeneity in the connected devices. There should be flexible security mechanisms are required to handle dynamic and heterogenic designs. In this paper, various security issues are represented along with the remedies.

Citation: Deepak Jyoti. "Security issues and their remedies in internet of things (IOT)", *2021. International Journal of Current Research, 13, (05), 17614-17618.*

INTRODUCTION

Internet has become important part of our life. People has become addicted of internet to communicate with other people. They are frequently exchanging information of any type with other people. Another one big platform has also introduced that is IOT. IOT is Internet of things. It is a wonderful platform where machines can communicate with each other, where machine can be controlled and operated remotely. Internet is the backbone of IOT.IOT is the field to create smart home, smart cities and smart everything to improve the quality of life of human beings and to reduce the operational cost. Internet of Things (IOT) is a worldwide network in which physical things are connected to the internet virtually. The success of IOT greatly depends upon a well-defined architecture which can provide scalablility, dynamic, and secure platform for its deployment. Each connected object has its unique identification. IOT is the latest emerging technology which is the way to interact with devices.

Corresponding author:** ***Deepak Jyoti,
Assistant Professor, PG Deptt. of Computer Sc. &IT Shanti Devi Arya Mahila College, Dinanagar.

In future, all electronic devices will be smart devices which can sense, compute and communicate with other hand-held and other smart devices. The major challenges in IOT are device heterogeneity, energy optimization, tracking capability and scalability. Many more challenges are there to focus and to find solutions to make IOT more efficient. The devices connected in IOT may be of heterogeneous type in the designing of IOT. The basic concept behind IOT is the presence of various wireless technologies around us like Radio-Frequency Identification (RFID) tags, sensors, actuators. Mobile phones, in which all wireless computing and communication systems are effectively embedded. Each embedded object has unique address. These objects interact with each other and reach at their common goals. These interconnected devices exchange information with each other as per user instructions and requirements. This is the future world where virtual and physical life is merged, where all embedded objects are interconnected and communicate with each other. The Integration, scalability, ethics communication mechanism and security are the major challenges. As the IOT is growing faster, everyday/every minute a new device is getting connected in this network. So scalability is increasing every time a new device gets connected.

There is issue to manage frequently increasing scalability. Most of the connected heterogeneous devices are battery operated. There is more energy consumption while communication. If the battery gets failure then communication will get fail. So there is need to optimize the battery consumption. Tracking of the smart connected devices must be identified and authenticated in no more time to avoid delay. It should all done automatically and self organized. There are main challenges as discussed but I will present detailed information about security issues in IOT. Security and privacy is the major challenge of IOT. Authentication and Identification of these inter-connected heterogeneous devices are the major reason behind security and privacy in IOT..All connected objects can communicate and accessible with Internet. Every connected device will have its own unique ID. These connected devices have the capability to sense, compute and communicate through internet. There is need of security management while connecting all hardware and software components in the IOT to get effective, efficient and secure connectivity. When IOT devices are connected with server then users can unknowingly introduce security vulnerabilities at the application layer. Any connected device can be hacked without security. Once hackers gain control, they can disturb the object's functionality and steal the user's digital data.

International organizations are making a lot of efforts to ensure data security and privacy in IOT design. Trust is very important in all online activities. When we all perform all activities on IOT then web user's sensitive information should not disclosed, it should be the responsibilities of the owner. For example consider the message and video clips of the operation on the ATMs or online banking towards the server, user have the trust in the bank for the security of their sensitive information, so that it will not be disclosed which can harm the user. When things communicate in an analogous manner, then trust of safe use of taxes will stop when one treats on Twitter trust must exist that no one will harm him/ her due to his tweet. As IOT is growing fast but simultaneously security and privacy issues are also growing very fast they are the big challenges for IOT.

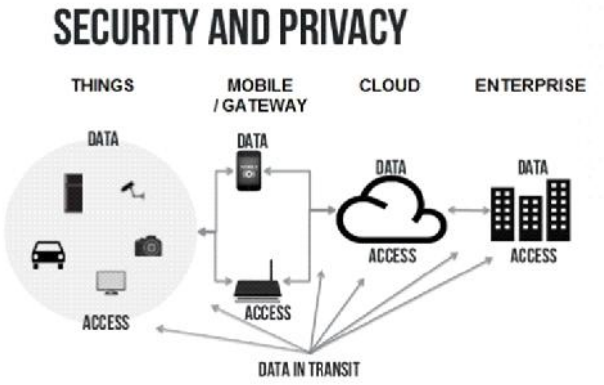
Security Risks

- IOT devices are connected to your handheld communicating devices then lack of security increases the risk of your personal as well as sensitive information also getting leak during all communicating process.
- The data is collected and transmitted to the IOT device. IOT devices are connected with consumer and provider network which again connected with other systems. If these connected IOT device have any security weakness then consumer network can get effected which can further attack other connected systems and damage them.
- Unauthorized user can exploit the security and can create risks to any type of safety issues.

Privacy Risks

- These IOT connected devices equipped with various hardware and software through heterogeneous devices so there are obvious chances of sensitive information leaking through unauthorized manipulations .
- All these connected devices may have stored the user's personal information such as name, address, date of birth, health card information, credit card detail and much more without encryption which is the sensitive data of user and can leak or hacked during transmission while communication.

So there are many security and privacy issues with IOT. IOT facilitates our lives which allow us to manage our daily routine tasks remotely and automatically.



Security is important for many communications for example ATM messages which should be communicated on secure internet. Any type of security tear and distortions can lead to serious issues. The smart cities security is also important. The city deploys smart health, public safety, transport and deploys IOT and smart home application and services. Many organizations have taken initiative for solving cyber security problem in smart cities. Privacy is very important. The video clips taken at smart home communicated on the internet application and if the clip reaches to unrelated entities then it can lead to a very serious problem of the home security. The rapid development of big data and IOT has brought convenience to people, and we also encounter unprecedented information security risks. The big data of IOT is stored in a server with a cloud computing platform. Cloud computing servers are distributed around the world. The diversity and complexity of the server determines that the user does not know where the data is stored, and the security risks exist. Cloud computing mainly uses virtual technology to achieve data sharing, and many virtual machines share one resource. With the advancement of internet and wireless communication, smart devices and things, and IP protocol and sensor network technologies, more and more network-based objects have been involved in IOT cyber security. The cloud computing platform does not guarantee the complete security of end-user information. The end-user is handed over to the cloud computing platform. Cloud computing platforms analyze and process data and have data access. In this way, the end-user doesn't have complete control over the data. In the process of calculating and processing data in the cloud, the data is easily leaked. IOT is a new technology and people are not familiar , not aware much about it. Most of the security issues are on manufacturing side, either hardware or software or network side. Unauthorized users and business processes users can create bigger threats. User's ignorance and lack of awareness of the IOT functionality is the biggest IOT security risks and challenges. As a result, everybody is put at risk. These IOT devices are operated automatically without human intervention. These devices should be secured from outside threats.

Every new threats or issues or vulnerabilities are discovered, immediately IOT system must be updated. Updates are also very critical. During any update, all data will be sent to the cloud. A hacker can steal any sensitive information from the unencrypted connection and unprotected files. Most traditional cyber security protection tools have focused on network and cloud. Endpoint and over-the-air (OTA) vulnerabilities are frequently overlooked. Bluetooth and WLAN are mature technologies which are used in many IOT applications but very little efforts has been done for the vulnerabilities of these devices. While there is a lack of universal IOT security standards, manufacturers will continue creating devices with poor security.

Security Issues in IOT: Not only we are connected to the internet, machines or things are also connected to internet. All these things are continuously communicating to each other. But this new technology is not matured, so it is not enough safe. IOT must have some security features for each of IOT architecture. The security problem may occur due to the technical problem and cyber ethics. Security means data should available to the authorized user. Data is interchanged between many users and devices. It is very much necessary to confirm the authorized user to deliver the data. It is also necessary to check the correctness of data to ensure that the same data is delivered what the sender has sent. Data should be delivered to authenticated device or user. Mutual authentication must be checked before communication. Data should be available all time whenever required. So availability, authentication, confidentiality, integrity and heterogeneity device management are the key principles of security in case of IOT. Some policies must ensure to manage security and transmission of data in effective way. Sensors embedded in the devices need to do encryption and decryption to secure the data. Security issues occurs on each layer of IOT architecture.

Four layered Architecture: There are many security threats which can occur on each layer of IOT.

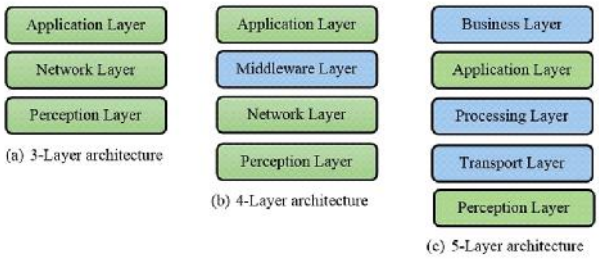


Fig. Layer wise Architecture

Perception layer has sensors which sense and gather information. It is the basically physical layer. This layer sense the physical attributes and sense other smart objects and then transmit the data. These sensor can get attacked by the owner of network or hackers or attackers. Actually these sensor run in outside environment. The confidentiality of this layer can be easily affected either by spoofing, timing attack or device capture attack. In case of device capture attack, device itself is hacked and seize all data from that device. Attacker may receive the encryption key and do the encryption within the time, it is known as timing attack. Timing attacks occur in in the system with weak computing capabilities. Attacker may hack the data and modify it and then resent it. Attacker can misuse the information.

All these types of attacks can send malicious data and threaten the integrity of data. It is also known as replay attack. Network layer is also known as transmission layer. It is in between perception layer and application layer. Data can be transmitted in wired form or wireless form. It create the networking among the smart objects. Its duty is to transmit the data. So it is highly sensitive layer where attacker can attack. It is further divided into two sublayers that is routing layer and encapsulation layer. Encapsulation layer forms the packets. Routing layer helps to transfer the packets from source to destination. Dos (Denial of Service) , Main in the middle (MiTM), storage attack, immoral attack are the common type of attacks in this layer. DoS is a type of attack in which make inaccessible the system or machine to the intended user by sending any irrelevant information. Storage attack is also a very dangerous attack in which data stored in cloud can be attacked and attacked data can be modified to incorrect data. MiTM is a attack in which attacker secretly intercepts and modify the communication between sender and receiver attacker can also gain the control of the system by immoral attacks.

Application layer is the layer in which all applications which are used by the IOT. It may be smart city, smart home, smart anything. It is the layer to provide all services to applications. Type of services depends upon the information collected by sensors. IOT is used to make anything smart. There are many security issues at this layer there are many malicious software which can attack on application layer. That code can destroy the whole system. It is a type of threat which cannot be stopped to do any malicious activities. Cross site scripting is a type of injection attack which enable attacker to attack on client side script like java script. In this attacker can change the content of original information. Support Layer is introduced in the three layer architecture of IOT to improve the security. When the data is sent to the network layer directly in case of three layer architecture, there may be more threats. To avoid this, new layer is introduces as support layer. Information is sent to this new layer which is obtained from the perception layer. It protect the user from threats. It also verifies that sent data is authentic. To verify the authentication, it uses passwords and secret keys. It also send information to the network layer. Information can also attacked by unauthorized access and malicious insider attacks. Malicious insider attack in which the authorized user can steal the information of other user.

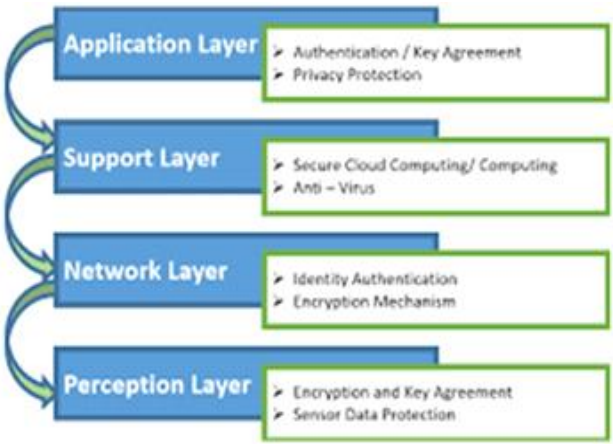


Fig. Four Layered Architecture of IOT with Security Mechanisms

Five Layered Architecture: There were some security issues and threats in the four layered architecture. To solve this, new five layered architecture introduced. It introduced two more layer in the three level architecture, the name of introduced two new layers are business layer and processing layer. Processing layer is the middleware layer. It collect information from transport layer and process it to extract the useful information and eliminate the extra information. There are also some attacks which can affect the performance of this layer. Exhaustion and malwares are the common attacks on this layer. Exhaustion disturb the processing of IOT. Malware attack the confidentiality of information. It is type of virus, spyware, worms. They are type of executable codes to steal the information. DoS attacks sends the victim messages about unavailable network. Its aim to exhaust the resources of the system. It is easy to protect it by implementing protecting mechanism. Business layer introduced in the five layer architecture to manage and control all applications of IOT. The privacy of user can also be managed by this layer. Weakness in this layer allow the attacker to misuse the application. Any weakness in the application can create many security issues. There are many drawbacks in the business layer such as improper programming, improper validations and passwords. There may be security hole in the programming due to weak programming. Attacker can do anything in the system without the consent and knowledge of the user.

IOT Security Issues Remedies: IOT need security computes at all layers. Followings are the remedies for security in IOT.

- Secure all components: It is necessary to secure all components like hardware, software, third party components and network whatsoever are used IOT must be reviewed. They should be analyze to find out the weakness. If any issues detected, then it must be documented. If any weakness is detected then updation of the software is recommended.
- Secure both physical as well as digital environment: The core system should reside in internet server who is hosting.The facilities like backup power, diverse entry points, armed security, bio-metrics and many more are there which ensure physical and digital security at highest level. All edge devices should be designed with highest level of security-resistant methods. These devices must be designed with alert mechanism to avoid misuse or tampering of the system. Some automatic system must be used to protect the IoT system. Minimum set of authorization or permissions should given very carefully to the trusted party.
- Secure digital environment: Consider the nature of the communication between each component and select appropriate protocols for each type of communication. Data should be encrypted at all level. All communications should be verified for authenticity. Firewalls and other mechanisms should be used to secure the system. Find out all types of weaknesses of system and take all precautions and other security measures to overcome weaknesses of the system. Blockchain technology should be used for more security features, if possible. For core system components, private or dedicated network should be used to avoid or limit the external communications. All communications should be sanitized for both within the system and third party systems to avoid any illegal injection attack.
- Service Level Agreements: All services, systems, and components provided by a third party vendor or partner should be governed by a well-conceived Service Level Agreement(SLA). SLA should be according to service level expectations of the user. This document should also take the security of data of user and many other issues related to the data security and performance.
- Privacy of data: Proper segregation of data mechanism should be used to assure the privacy of data. As per need of user data should be available. Minimum set of authorization or permissions should given very carefully to the trusted party. Data should be partitioned in such manner so that unauthorized user cannot access other user data. User can see its own data only, not possible to see other user data. System manager and service provider should assure the consumer about the proper use of consumer's data as per the access rights and authorization. All efforts should be done regularly to maintain the privacy of system users. Auditing is very important to secure data. All applications and its updations which are distributed as service should be verified and registered as secure mechanisms.

Security features needs to be incorporated in a standard format recommended for IOT. For example a standard for electronic products architecture is from developing group EPC global. This group is responsible for creation and maintenance or privacy policy products. Open Web Application Security Project (OWASP) has undertaken the associated security issue of IOT for the purpose of helping developers, manufacturers and consumers it is open source and hassle free to use licencing policy. Project is community model based software development initiative. A community model is making collective efforts and initiative by universities, organisation an institution in an open source projects. OWASP has undertaken a number of security related sub projects such as ones for defining the top one ability, attack surface area and testing guides OWASP has identified top ten vulnerability in IOT application / services as follows:

- Weak, Guessable, or Hardcoded Passwords.
- Insecure Network Services.
- Insecure Ecosystem Interfaces.
- Lack of Secure Update Mechanism.
- Insufficient Privacy Protection.
- Insecure Data Transfer and Storage.
- Lack of Device Management.

Conclusion

IOT is the next step to Internet. We are using internet anywhere and anytime. IOT allows to connect people and devices (things) Anytime, Anyplace, with Anything and Anyone. This paper gives a brief idea about IOT, IOT layerd architecture security issues and their remedies in IOT. There are connectivity in heterogeneous objects, so presently there are many challenges. So this area has many open research issues. Security is the ongoing topic of research. Now a days, there are still many risks and security issues in IOT and many will be solved in coming research and many more issues will be introduced. A machine learning framework can be used to detect IOT attacks and solutions to the attacks. Machine learning can help to solve many issues in IOT. In summary, there is a major need of security and privacy in this

heterogeneous smart virtual or digital environment. The current security services are insufficient for complex communication technologies. The future research directions may consists of many more challenges and security issues faced by IOT.

REFERENCES

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol.29

Zanella, A. N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things* J., vol. 1

Elmaghraby A. S. and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," *J. Adv. Res*., vol. 5

Sicari, S. A. Rizzardi, L.A Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead*", Comput. Netw*.

Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I.: Internet of things: Vision, applications and research challenges. Ad Hoc Networks (April 2012) 1497–1516

Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* 2015, *17*, 2347–2376. [Google Scholar] [CrossRef]

https://innovationatwork.ieee.org/how-to-make-IOT-batteries-last-longer/

Yang Lu, Member, Li Da Xu, "Internet of Things (IOT) Cybersecurity Research: A Review of Current Research Topics" https://ieeexplore.ieee.org/abstract/document/8462745

https://www.ijedr.org/papers/IJEDR1701065.pdf

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453/

https://www.researchgate.net/figure/Definition-of-IOT-21-The-four-layer-architecture-is-like-the-three-layer-architecture_fig1_349426656

****