Internet of Things (IoT) Security is more Than a Trend

Prathyusha Bankupalli
Bsc Computers, Electronics
Gayatri College of Science and Management
Srikakulam, Andhra Pradesh, India

Abstract:- The Internet of Things is the combination of technologies with physical devices for communication and intelligence or interaction with internal and the external environment. The Internet of Things refers to machine-to-machine communication rather than human-to-human communication. it's a transformative force shaping our future. By connecting devices and enabling data-driven decisions, IoT is revolutionizing industries, unlocking new opportunities for innovation, and driving unmatched efficiency. Embracing IoT means embracing a world of interconnected possibilities and boundless potential. Security is one of the finest issue that need to be addressed when we are implementing smart systems in to the industries. This article provides over view on security for different layers of IOT systems in usage.

Keywords:- *Internet, Devices, Efficiency.*

I. INTRODUCTION

Internet of Things (IoT) a pattern of approach that enables communication of electronic devices and sensors that will make our lives easier through the internet. The innovation that brings together many smart systems, infrastructures, smart devices and sensors. The concept aims to connect anything with anyone anywhere irrespective of time. The popularization of IoT devices and technology in our daily life has changed a lot. One of the developments in the field of Internet of Things is the concept of smart homes, which include the management of internet devices, home electronics [2]. Smart Health Sensing System is one of the sectors where IOT plays an important role. SHSS uses intelligent systems which help in supporting health for humans. These can be used irrespective of the checkup areas to monitor the health issues [3].

II. HOW IT WORKS

The functionality of IOT consists of 5 different layers. These are perception, network, middleware, application and business layers. The perceptual layer contains devices like sensors, chips and other objects that connect to the IOT network. These collect the information and pass them to the network layer. This passing of information to network layer may use Wi-Fi, Bluetooth etc. The middleware works in decision making and generating results by computing. The entire device management is performed in application layer on top the business layer controls the application layer and with services it provides. The business layer is used for visualization of the information that was received and uses it for future strategies. IOT consists of different blocks and activities such authentication, sensing, identification and management. Fig 1 explains about the architecture layers of IOT.

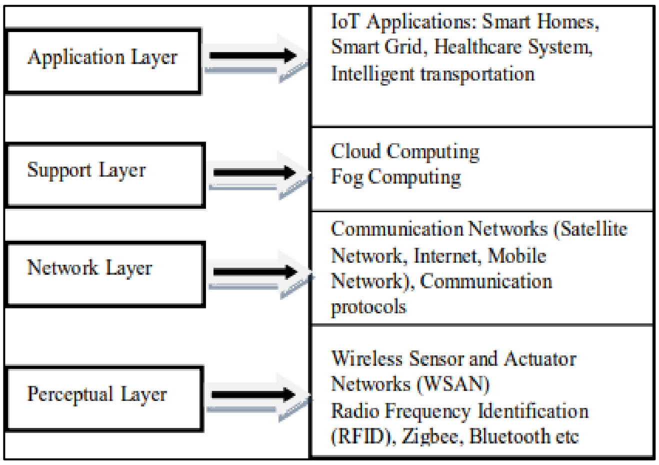
Application Layer
IoT Applications: Smart Homes, Smart Grid, Healthcare System, Intelligent transportation
Support Layer
Cloud Computing
Fog Computing
Network Layer
Communication Networks (Satellite Network, Internet, Mobile Network), Communication protocols
Perceptual Layer
Wireless Sensor and Actuator Networks (WSAN)
Radio Frequency Identification (RFID), Zigbee, Bluetooth etc

Fig 1. Explains about the architecture layers of IOT.

III. SECURITY

There are security techniques such as device authentication, access control methods were used to improve IOT security. Security and privacy are the crucial and important aspect that has to be focused up on. Security attacks in health care where IOT plays important role can cause loss of many lives and in business industries it may cause financial losses. Security is measured and provided very cautiously to all the layers that contribute for implementation of smart devices.

➢ *Perceptual Layer*

As they consist of devices like sensors, chips and other network connecting devices there are chances for more cyber-attacks. Some of them are deployed in open fields and have possibility of physical attacks which lead to mislead the sensitive information and get access to the node. This can be through below possibility ways:

- Fake Node: Attacker may add fake node and collect the data which reduces power of the device
- Physical damage: In denial service these devices may get attacked physically

- Code Injection: Attackers can take access to the system by implementing illegal code to the node to get the sensitive information
- Mass Authentication of Nodes: Many nodes face authentication issues for network communication which affects the performance

These are some of the security issues that can be faced in perceptual layer. These can be reduced by securing the systems from physical access. Authentication is necessary to prevent unknown access to the systems.

➢ *Network Layer:*

There is sufficient protection provided to network layer but there are some issues which need to be addressed like Man in middle attack, Dos attack are still affecting the networks.

- Denial of service: Overburdening the network with traffic beyond its capacity which results in unavailable network for useful services.
- Routing attacks: The routing information can be altered and creating the routing loops, false routes and dropping network traffic [5]
- Network Congestion: Large amount of data with communication caused by many devices authentication can cause network congestion issue. This can be addressed by authentication mechanisms.

Advancement is needed in network communication to resolve these routing attacks, network congestion and other network security related issues.

➢ *Application Layer:*

Security at application layer may not be same it varies from application to application as per the requirements. Data sharing is one of the common aspects in application layer. Data privacy and protection with access control are need to be focused in this particular layer.

- Data authentication: One application may have many users with multiple access proper authentication and access controls are required to protect data in this application layer.
- Malwares attack: Attackers may steal and mislead the data and the services that are involved in the system.
- Phishing Attacks: Attackers may use infected mails and weblinks to take the credentials for accessing the sensitive information

To protect the application layer strong authentication and access control are required. Having strong password can also resolve this issue. Anti-virus can help in reducing these challenges in the systems.

IV. CONCLUSION

Further attention and research is required for improving the security for different layers of IOT systems. In this survey article we provided how internet of things is involved in our lives and how it works with in layers involved in providing and improving the security for different layers. We discussed the challenges that are involved and measures that needed in resolving the security level issues in perceptual, network and application layers. Important application arears of IOT are mentioned in this article.

REFERENCES

[1]. Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitoredand controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.

[2]. Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag. 2017;55(1):26–33. https://doi.org/10.1109/MCOM.2017.1600363CM

[3]. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw. 2018;4(1):118–37.R. Nicole https://www.sciencedirect.com/science/article/pii/S2352864817300214?via%3Dihub

[4]. Ali I., Sabir S., Ullah Z. Internet of Things security, device authentication and access control: A review (2019) arXiv preprint arXiv:1901.07309

[5]. D. Wu, and G. Hu, "Research and improve on secure routing protocols in wireless sensor networks." In Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on, pp. 853-856. IEEE, 2008