IJIRMET
ISSN (Online): 2456-0448
International Journal Of Innovative Research
In Management, Engineering And Technology
Available online

A TOP-DOWN SURVEY ON SECURITY ASPECTS OF THE INTERNET OF THINGS(IOT)

Divya James
Research Scholar, School of Engineering,Avinashilingam Institute of Home Science and Higher Education.
divyajames@gmail.com

Alagusundari.N
Research Scholar, School of Engineering, Avinashilingam Institute of Home Science and Higher Education
alagusundari124@gmail.com

Dr.TKS Lakshmipriya
Professor, School of Engineering, Avinashilingam Institute of Home Science and Higher Education
tkslp.dr@gmail.com

To access & cite this article
Website: www.ijirmet.com

ABSTRACT

Internet of Things (IoT) is becoming the most significant computing platform. With recently developed applications such as Smart Transportation, Smart City, Smart Home, IoT technologies are significantly changing our lifestyle. Novel Solutions are essential to protect the IoT systems from the attacks. The objective of the Internet of Things is to provide security and privacy to the users. This paper aims to analyses security challenges resulted from the characteristics of IoT systems. It also discusses the attacks and open problems in different layers. Finally, it analyses the impact of IoT security in smart home appliances.

KEYWORDS : IoT, Security, Attacks, Smart Homes

I. INTRODUCTION :

IoT (Internet of Things) comprises of a network of physical devices,vehicles,home appliances and other items embedded with electronics,software,sensors,actuators and network connectivity which enables these objects to get connected and exchange data.

IoT is also an Internet Technology connecting devices, machines and tools to the Internet using wireless technologies like Bluetooth, WiFi, Zigbee.

IoT[1] results in the unification of technologies such as low power embedded systems, cloud computing, big data, machine learning and networking.The two solutions for the networking technologies are either to expand the existing network or to build a separate system from scratch. IoT works on four differentcomponents, and it is depicted visually in Fig1.

SENSORS

Sensors are devices used to collect data from the environment.

IOT GATEWAYS

IoT Gateways acts as an intermediate node to collect data from the end devices and transmit it to the internet.

CLOUD/SERVER INFRASTRUCTURE

The data collected by the sensors have to be stored and processed intelligently within the cloud infrastructure.

APPLICATIONS

Applications will support the end users to control and monitor the smart devices from remote locations.

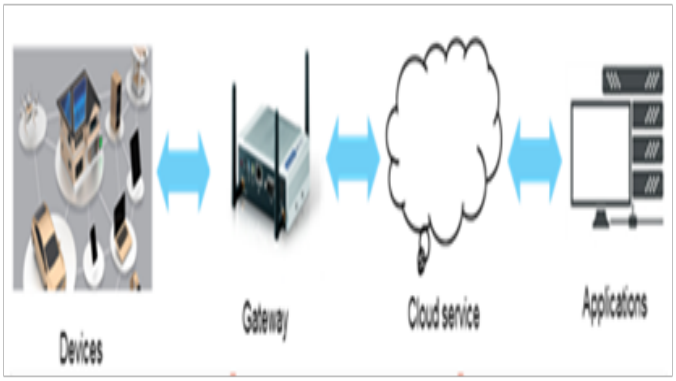

Fig1: Environment Diagram

Applying security mechanisms in an IoT system is more challenging than with a traditional network, due to the heterogeneity of the devices and protocols as well as the scale or the number of nodes in the system. The challenges in applying IoT security mitigation which is due to physical coupling, heterogeneity, resource constraints, privacy, scalability, trust management and unpreparedness for security.

II. THE NEED FOR SECURITY IN IOT :

THE DIFFERENT LAYERS[2] OF IOT CONSIST OF:

Perception layer

Aforementioned is the physical layer for sensing and collecting information from the environment.

Network layer

This layer transfers the sensor data from the perception layer to the next layer and vice versa through the networks.

Application layer

This layer is responsible for delivering application-specific services to the user. It defines various applications that can be deployed using IoT. Each layer has its's security[3] concerns:

PERCEPTION LAYER SECURITY PROBLEMS:

The primary technologies used in the perception layers are WSN, RFID and other types of sensing and identification techniques. Frequent attacks of the perception layer are:

Node Capture

The nodes which present at the network gateway are more likely to be compromised which might result in the leakage of relevant information which endangers the security of the entire network.

Fake Node and Malicious Data

The adversary adds a malicious node to the existing system through which they can circulate malicious codes and information over the network, thus infecting the whole system.

Denial of Service Attack

DoS and DDoS attacks are the most common and vicious attacks over a network. These attacks lead to depletion of network resources and unavailability of service.

Replay Attack

The adversary replays a previous message to the destination node to compromise the network trust and authentication schemes

.

Network layer security problems: Threats to most common security services like confidentiality, integrity and availability may happen at the network layer. Attacks like eavesdropping, Man in - the middle, DoS/DDoS, Network Intrusion are common threats at this layer.

Heterogeneity:

Due to the use of different technologies and protocols security and network coordination is hard to maintain. Thus, making the system vulnerable.

Scalability Issues

IoT comprises of a large number of devices, and more devices may enter or leave the network at different times which raises issues like lack of authentication, network congestion etc. It also depletes a lot of resources.

Data Disclosure

By using social engineering techniques the adversary might be able to obtain sensitive information from the network. As these devices collectively have vast amounts of data, using specific data retrieval techniques, it is easy to extract information from the nodes.

Application layer security problems This layer needs different security standards as per the application requirements, which makes the task of securing the application hard and complicated. Some of the security and privacy issues at this layer are :

Mutual authentication and node identification

Each application has a different set of users which require various degrees of access privileges. Thus, to prevent any illegal access effective authentication schemes should be applied.

Information Privacy

User privacy[4] plays a significant role in each communication. Sometimes the techniques which are being used to process data might be vulnerable which leads to data loss and over a long term can do considerable damages to the system.

Data Management

Due to substantial data collections, the system complexity increases which require a lot of resources and sophisticated algorithms to manage data and may also result in data loss.

Application Specific Vulnerabilities

While developing modules for an application some vulnerabilities might be left behind which are unknown to the user. These can be exploited by the adversary later on.

III. CASE STUDY :

SMART HOME TECHNOLOGY

Smart Home is becoming increasingly popular recently [5]. Gartner's IT Hype Cycle 2016 Report identifies that smart connected home is an emerging technology. By 2022 a typical house could contain 500 or more intelligent devices. Smart Home has the vision of adding intelligence to everyday home objects, such as appliances, door locks, surveillance cameras, furniture, garage doors, and so on and making them communicate with existing cyber-infrastructure. The addition of intelligence to physical objects offers many benefits to better human lives, including increased convenience, safety, security, and efficient usage of natural resources. For example, the Smart Home can adjust the blinds to save energy based on the environmental changes, automatically open the garage door when it senses an authorised vehicle approaching, or automatically order medical service when an emergency is detected. In Smart Home, traditional physical home devices become a part of the extension of the existing Internet. The consequence can be severe if the machines compromise. For example, successfully hacking smart lock will enable strangers to enter the house; compromising of baby monitors can scare babies remotely by strangers; hacking microwave can cause a fire at home. Owners of Smart Home may not want to live in Smart Home if security is a concern. Instead, they may expect to improve the safety of the house by using smart surveillance services. However, continuously collecting data from Smart Home devices can reveal private activities of homeowners as indicated in [6,7]. It poses severe threats to the homeowner's privacy.

Fig 2: Smart Home Devices

Smart home controller like cell phones are used to control and manage the devices[8] using IoT. Most the appliance in the kitchen are smart, example like refrigerator, microwaves, dishwasher etc. In the living room starting from the smart TV, it goes on with a smart lighting system. IoT plays a major role in connecting all the smart systems with a controller. Then the ways and the services provided are discussed.

ALGORITHMS AND METHODS

The interactive home environment is being created by different algorithms and methods. Artificial Neural Networks are used to detect and recognise the resident's pattern. Another model of the neural network is human behaviour modelling. Neural networks are popular because they don't require prior knowledge about the systems.

Distributed intelligent systems are multi-agent systems, which cooperate by sharing knowledge. Each agent is responsible for its domain area. Hence health monitoring from remote is made possible.

Bayesian statistics also helps in developing remote access of the inhabitant's locations and their conditions. These methods use the last known sensor state to improve the accuracy of the location prediction. They also use the immediate state to predict the future.

Case Base Reasoning and prediction algorithms make decisions. Context awareness can be achieved by these algorithms. Active Lezi and other predictive algorithms work the previous history for predicting the next activities. Recent changes in the user's behavior are also considered by the systems. Fuzzy logic is far better than the binary logic in controlling the home appliance. Fuzzy logic uses multi-valued logic for reasoning. Recent changes in user behavior will also reflect in the system.

Finally, image processing methods also help in human activity recognition. The skin colour of the face and hand tracing helps to do the process of image processing. The future smart home is likely to adopted image processing. Intelligent homes are devoted to provide safety and comfort for older adults.

The above discussed algorithms and methods used in smart home applications is given in the table below.

Table 1: Algorithms and Methods used in smart homes

Algorithms and Methods	Purposes
Artificial Neural Networks	Predicts the future states of home
Detects the daily activities	
Distributed intelligent systems	Health monitoring
Hidden Markov model	Behavioural model created
Bayesian Statistics	To determine the location
Summarization algorithm	Changes in the system are tracked
Statistical Predictive algorithm	Predict the daily life activities
Active LeZi Data compression	Predicting the next activities
Case Base Reasoning	Makes decisions based on the previous state
Fuzzy logic	Home appliance control

SMART HOME UTILITIES AND SERVICES

Smart home technology has significant improvement in health care like patient monitoring[9,10], telemedicine, and wellness monitoring. Smart home keeps on tracking the user's state and generate an alarm when an abnormal vital sign is detected.

Table 2 represents the summary of smart home utilities and services. The smart home is providing a wide range of services which provides satisfaction for the consumers. Additional research has been required for service to be cost-effective, efficient and acceptable.

Table 2: Smart home utilities and Services

Services	Functions
To provide comfort	Lighting, temperature
According to the resident's desire	
Remote access monitoring	Appliance monitoring and controlling via mobile phone and computers from distance location
Automate the home appliance	Voice operated home appliance
Wellness monitoring	Support elderly and disabled persons from remote locations

One of the main aims of the smart home is to reduce the interaction between the user and the devices. As discussed smart homes can control parameters like light, temperature, according to the user's choice.IoT helps develop a smart home with intelligence of what next to be done.

IV. CONCLUSION :

Smart home technology is increasing because of industrial demand. The work explains the attacks and challenges in different layers of IoT.Also it gives a general view on the algorithms and methods used for the smart home and its utilities. In the future smart home and the IoT are becoming the centre of intelligent services.

V. REFERENCES :

1. Mardianabinti Mohamad Noor, Wan Haslina Hassan, Current research on Internet of Things (IoT) security: A survey,Computer Networks 148 (2019) 283–294
2. K.Sha,W.Wei,T.Andrew,Yang,Z.Wang,W. Shei,On security challenges and open issues in Internet of Things, Futur. Gener. Computer. Syst. 83 (2018) , 326-337
3. A.Tewari,B.B.Gupta,Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, Futur. Gener. Computer. Syst. 83 (2018) , 1-13
4. Tianyi Song, Ruinian Li, Bo Mei, Jiguo Yu, Xiaoshuang Xing, and Xiuzhen Cheng, A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes, IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 6, DECEMBER 2017.
5. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, 2019. "The Influence of 'Adventure Tourism Activities' in promoting tourism business in mountain stations", African Journal of Hospitality, Tourism and Leisure, Volume 8 (2).
6. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, Nov 2018. "A Study On consumer satisfaction and preference of colour TV brands in Chennai city", International Research Journal of Management and Commerce, Volume4, Issue 10.
7. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, "A Study on Attrition: Turnover intentions of employees", Jan 2019. International Journal of Civil Engineering and Technology (IJCIET), Volume 10, Issue 9.
8. Dr. S. Rabiyathul Basariya, and Dr. Nabaz Nawzad Abdullah, Dec 2018. "A STUDY ON CUSTOMER'S SATISFACTION TOWARDS E-BANKING", International Research Journal of Management and Commerce, Volume 5, Issue 12,
9. Dr. S. Rabiyathul Basariya, "A study On Customer Satisfaction towards Shopping Malls", International Journal of Business Intelligence and Innovations, Volume 1, Issue 2, special edition Oct-2015.F
10. A.Jacobsson, P. Davidsson, Towards a model of privacy and security for smart homes, in Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT2015),2015.
11. I.Rouf, et al., Neighborhood watch:Security and privacy analysis of automatic meter reading systems, in Proceedings of 2012 ACM Conference on Computer and Communications Security, 2012.
12. NicoSurantha,WingkyR.Wicaksono,Design of Smart Home Security System using object recognition and PIR Sensor, Procedia Computer Science 135 (2018) 465–472
13. Seungyong Yoon and Jeongnyeo Kim.

Remote security management server for IoTdevices,International Conference on Information and Communication Technology Convergence (ICTC),IEEE Conference Publications,2017

14. Shih-Hao Chang, Rui-Dong Chiang, Shih-Jung Wu, and Wei-Ting Chang,:A Context-Aware, Interactive M-Health System for Diabetics, IEEE Computer Society, (pp. 14-22), May-June 2016
15. Hammi M, Livolant E, Bellot P, Serhrouchni A, Minet P. A Lightweight IoT Security Protocol. In1st Cyber Security in Networking Conference (CSNet2017) 2017 Oct.

