ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 9| Issue: 9| September 2023|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2023: 8.224 || ISI Value: 1.188

SECURE SMART HOME DESIGN AND ANALYSIS FOR ELDERLY PEOPLE USING INTERNET OF THINGS (IOT) TECHNOLOGIES

Dr.D.Devi Aruna
Associate Professor,Department of Computer Applications, Dr.N.G.P. Arts and Science College,Coimbatore

ABSTRACT
The Internet of Things technology is used for increase the old people living securely in environment of smart home and assist their caregivers. The smart homes are developed with automation of appliances and activities monitoring. The goal of smart home is to assure home resident safe. To increase the elder safety by using the IoT sensor and detect the attackers. The anomaly detection system is the system which identifies the interruption of network and computer by observing the behaviour of the system. This research paper analyzes and detects the behaviour of abnormal. This report discusses the system of anomaly detection based smart home from the perspective of security. The secure model of smart home is developed using Cisco packet tracer and device of IoT network is simulated and analysed the result.
KEYWORDS: ***Smart home secure, IoT technologies, detection system of anomaly detection, system for intrusion detection.***

I. INTRODUCTION

The goal of smart home is to assure safe for home resident. To increase the elderly safety by using the IoT sensor and detect the attackers. The detection system of anomaly is the system which identifies the interruption of network and computer by observing the behaviour of the system. The system of anomaly detection is a system identifies the attackers in the network. The expansion of Internet of Things is network of internet into physical devices which is regular. Over the internet the devices of IoT are connected and controlled and remotely monitored. The devices of IoT architecture based on the system of anomaly detection consist of four different layers. The layer perception contains various sensors like RFID and code of QR for the data collection like pressure, temperature and humidity. The data collection is done by the sensor and sends to the next level, when actuator gets command for control for the specific actions performance. The layer of network contains the communication of software is incharge of data transmission acquired from the sensor of various layers. The layer of internet which includes the aggregation of data and control. The layer of middleware breaks huge data and processes. In the processing layer processing of big data and computing of cloud is done. The responsibility of application layer offers the user services based on the requirement. These layers are prone to possible attack. The sensor data which is in real life is acquired form household of elderly people using the doors, windows and sensors to help for the detection of abnormality in the sensor data. This report discusses the system of anomaly detection based smart home from the perspective of security. The secure model of smart home is developed using Cisco packet tracer and device of IoT network is simulated and analysed the result. (ManojNair, 2018).

II. RELATED WORK

In the current years, great rise in smart homes because of the addiction in technology. Smart home have designed to enhance the life quality for every people, particularly normal nondisabled person. The smart home idea is for energy saving, lights control, heating control, air condition, locks door and coffee makers when comfortable of people. But peoples have disabilities will not able to benefits of smart home devices. The devices controlling when you setting using technology of smart home is a high quality help for people who are disabled physically and persons older. The disabled people problem is solved by using the control system based appliance of smart home for physically disabled people (adam, 2018).

Smart home can help the people with services of health care and social support. The people have the positive approach for the implementation of smart homes. Furthermore, the people were concerned in the system of health monitoring lead them to live alone. But at the same time, they were having the same problem on the data privacy so that the smart home provides security. The smart home assists the people to decrease the loneliness and medicine rememberness. The smart home have many advantages they are sensor efficiency, system of surveillance and personal misuse or information which is confidential taken into consideration. Furthermore, people have a data can be altered in media of communication by the adversary and sent to the cloud. The sensors are weakness to have attacks in the entire system. The adversary read the data against the security (Shemsi, 2018).

The approach for graph based using the GBAD tool for the anomalies detection living in the smart homes without the daily activity of residents interfering and decrease the healthcare cost with the situation. The smart homes are developed with automation of appliances and activities monitoring.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 9| Issue: 9| September 2023|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2023: 8.224 || ISI Value: 1.188

The behaviour of anomalous to be the spatial and anomalies of behaviour. The two theories are proposed which is approach of graph based is reliable for the anomalies detection in the smart home and exposed anomalies are potential syndrome of abilities of cognitive impairment. The system of anomalies detection assists the caregivers of patient and monitors the people and increase the independence of patient to perform the regular task and safety routine. This system setup by sensor installation all over the home for gathering of data about the activities of patients without routine interfering (Dey, 2019).

The anomaly detection system is the system which identifies the interruption of network and computer by observing the behaviour of the system. (Alfarsi, 2017).

III. SIMULATED ENVIRONMENT

The secure model of smart home is developed using Cisco packet tracer and IoT devices in the network is simulated and analysed the result. The simulation environment with case study is analysed to identify how to secure the smart home. Many hospitals use the system of anomaly detection in the smart home for the patient monitoring and health tracking. The smart home use the technologies of IoT and collection of data are sent to the cloud for the abnormal behaviour detection. The systems are connected to the internet and come with various threats and risk make unsafe to live people alone. Due to the vulnerability of smart home the people dies when the attacker's stops sensors and data prevented from the reach of hospital. The attacks in the network are denial of service, man in the middle and spoofing of RFID can be extended to the security risk in the cloud with the data exposures by the unauthorised users

IV.RESULTS

The smart home system consist of smart devices have sensor for activities recording of the residents in the home. The activities like smart door opening represents time spending in the room, smart light switch turning on represents the hours of sleeping.

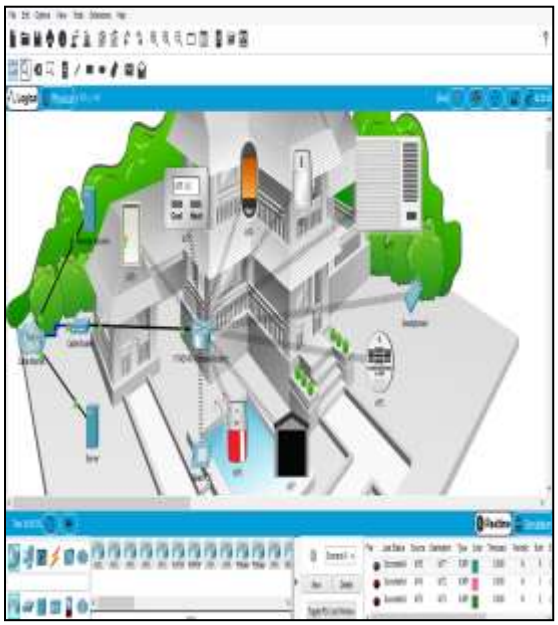

Figure 1: IoT Device Setup

After sensing the devices. Data transfer is real time collected by the sensors to the cloud compared to user normal behaviour. When the detection of abnormal activities, the caregiver of the people is notified.

Figure 2: working of IoT device

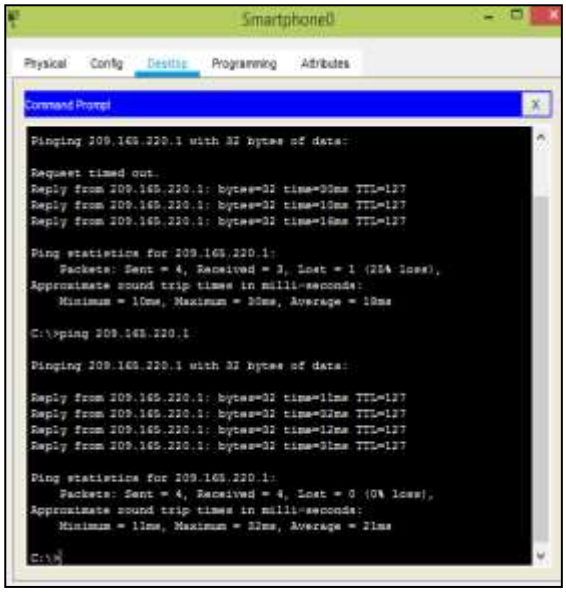

Figure 3: Ping Status of Devices

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 9| Issue: 9| September 2023|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2023: 8.224 || ISI Value: 1.188

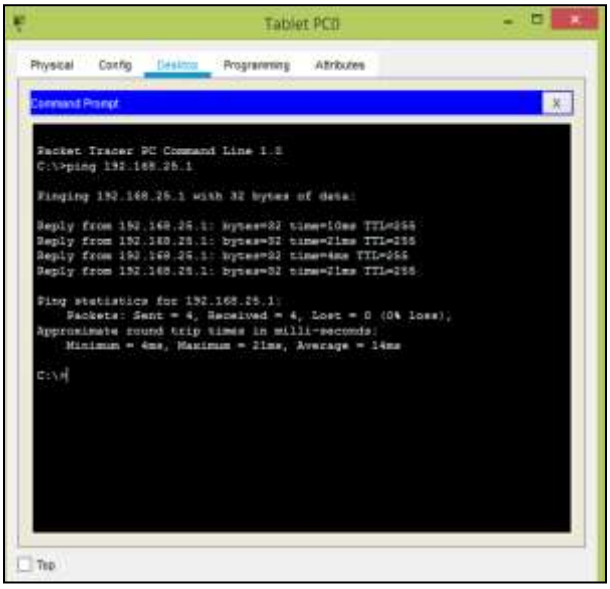

Figure 4 : Devices Ping Status

V.SECURITY CHALLENGES

The security threats are identified in the review of literature, the network layer processing is risk due to attacks. When the transmission of data is weakness due to attacks like DoS, spoofing of RFID and sinkhole. The smart home uses IoT technologies and data collections are sent to the cloud for the abnormal behaviour detection. The systems are connected to the internet and come with various threats and risk make unsafe smart home to live people alone. Due the vulnerability of smart home to attack which is internet based, the people die when the attacker's stops sensors and data prevented from the reach of hospital. The attacks on the sensor network are denial of service, man in the middle and spoofing of RFID can be extended to the security risk in the cloud with the data exposures by the unauthorised users. The smart home security is provided by using Access Control List. ACL is set up for the authorisation that can access and assured the information privacy in the framework of IoT. Access Control List can permit and block the request access from the various users in the system inside and outside. The ACL address the issues of authentication and authorisation in an environment of smart home based IoT.

CONCLUSION

This research paper investigates and detects the abnormal behaviour. This report considers the anomaly detection system based smart home from the viewpoint of security. The secure model of smart home is developed using Cisco packet tracer and IoT devices in the network is simulated and analysed the result.

REFERENCES

1. *Adam, S. (2018). Review of Cyber-Physical System in Healthcare. International journal of distributed sensor network , 6 (1), 321-328.*
2. *Alfarsi, G. (2017). Using Cisco Packet Tracer to simulate Smart Home. International Journal of Engineering Research & Technology , 6 (2), 321-329.*
3. *Dey, N. (2019). Medical cyber-physical systems: A survey. Journal of Medical System , 2 (3), 765-769.*
4. *ManojNair, l. (2018). Medical Cyber Physical Systems and Its Issues. International Journal on Advanced in computing , 5 (2), 219-228.*
5. *Shemsi, I. (2018). IMPLEMENTING SMART HOME USING CISCO PACKET TRACER SIMULATOR. International Journal of Engineering Science Invention Research & Development , 6 (1), 675-679.*