Smart Home Applications based on IoT

Sanjana[1*]

[1*]Department of Computer Science and Engineering, Amity University, , Noida, 201303, Uttar Pradesh, India.

Corresponding author(s). E-mail(s): sanjanachhawdi312@gmail.com;

Abstract

IoT is an integration of heterogeneous electronic devices as one, allowing them to communicate among each other. It is an integral part of many other industries, smart home being one of them. Smart home technology considered as primary service of IoT, had a fair share of growth from the beginning of the decade, while huge potential in today's date. Amid all the advantages offered by it, privacy and security of users remains the biggest issues for developers to tackle. However, different approaches are applied by many companies to combat this issue, to utilize its importance to the fullest.

Keywords: Internet of Things, Smart Home, security and privacy

1 Introduction

The concept of IoT was first introduced to the world in 1982, when a first modified internet connected Coke machine was developed. However, it was 1999 when the term was suggested. During work in Procter and Gamble, Kevin Ashton described it as the connection between internet and machine through sensors. IoT is a communication network between the electronic devices or in larger systems it functions as a single or central machine. This network converts billion of data, obtained from various devices that we use in our daily lives, into usable information. It focuses mainly on machine-to-machine communication, rather than machine to human. The Smart Home is an assimilation of different technologies and services using home networking for better life quality. In recent years, a vast advancement is observed in the use of smart

household devices all around the world which helped the markets to mature and progress with some pace. The rapid diffusion of sensing technology, advertisements power of big enterprises and media plays an important role in its development.

2 Internet of Things

Internet of Things refers to a network of appliance, where all things are solely and specifically addressed, determined and controlled by the computers. It is a collection of technologies and components such as sensors, actuators which allows them to connect with the internet, intercommunicate and connect with external environment.[1]

2.1 Applications of IoT

IoT has found uses in other fields such as medical and healthcare, environmental monitoring, manufacturing, transportation, media, building and home automation, energy management and many others as shown in figure 1. Some of them are:

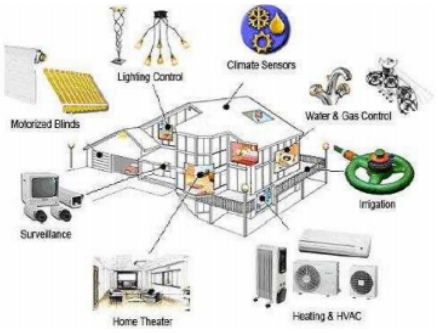

Fig. 1 Smart Home integration services[2]

1. Public Security services- IoT is used in security services for monitoring using sensors and controlling through smartphones and other devices. It also helps in intelligent monitoring.
2. E-health- In health sectors, it assists in supervision of the health and time management of a patient. For instance, household medical devices like sphygmomanometers are accessed by the network of IoT and community hospitals.
3. Data services- A large amount of data about various topics like games, movies or others can be stored and checked continuously.
4. Smart buildings and homes- IoT is an essential element of the smart homes and buildings. Many gadgets can be controlled efficiently and concurrently

from some distance away from sources. This area is expanding continuously and has a lot more scope in the upcoming time.

5. Enhanced learning- It also has some features like real-time monitoring, keeping in check progress report and comparing it from time to time and accessible learning materials for students. Hence E-learning gives a better environment for students to learn with according to their own pace and comfort. In Covid era, E-learning got boost and currently bringing revolution in learning system.

3 What is a Smart Home system?

The smart home is an environment, where heterogeneous electronic devices and appliances are networked together to provide smart services ubiquitously to individuals.[3]

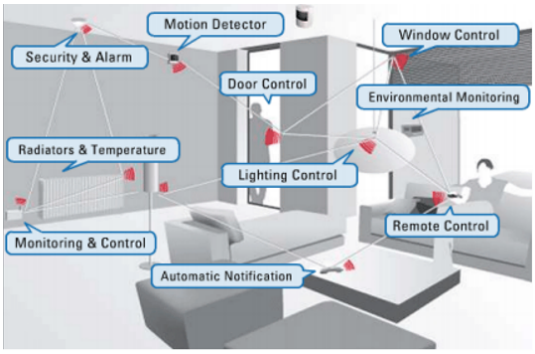

Fig. 2 Examples of the Smart devices[2]

3.1 Elements of Smart Home

1. Sensor surveillance- Sensors are used to monitor factors like temperature, humidity, fire, sound, light, closeness, etc in home.
2. User interface devices- User interface devices are referring to be the devices that provide a connection between humans and machines for communication purposes. For example, Remote control, computer, smartphones, tablet.
3. Networking- There are four types of carrier modes to transfer data namely, power line, wireless, wired and internet protocol. There are two types of networking that are possible in a system- wired network or wireless network. For example, wired devices such as fibre optic, coaxial cable and wireless devices like Bluetooth, Infrared, ZigBee, WIFI and RF.
4. Centralizing control is the one that is responsible for managing the execution of other devices. For example, Microcontroller, PLC, computer, FPGA.

3.2 Challenges

1. Security- Nowadays, one out of two devices is connected to the internet. As the number of connected devices increases, system security decreases. This issue will be discussed in more details in the later sections.
2. Availability- The availability of smart home appliances is limited and scattered because of their high costs. With the broader consumer market, prices can be pushed for making it available to more mass.
3. Signal interference- Sometimes, wireless devices can cause interference in the signal. Signal interference causes data and energy loss, as a result increases energy demand and cost.
4. Not user friendly for a certain group- Due to its complexity, some groups such as disabled, elderly and infirm people of people find it difficult to operate. IoT can bring many benefits for disabled persons if this problem is solved.

3.3 Benefits

1. Centralization- Centralized is a primary feature of smart homes. It allows different devices or network to be controlled and monitored from one single device.
2. Real-time monitoring and control- Data is both sent and received from IoT devices and sensors for monitoring and controlling the gadgets.
3. Remote access-The automated appliance control enables users to execute tasks before arriving home. Therefore, also saves the time of the user. The remote system is found to have an efficient performance in real-time responses.
4. Assistance- It provides the solution for assistive technologies especially to the disabled and elderly person. With more renovations in this area in the future, it can prove to be a strong support for them.
5. Manages energy consumption- It is an area with lot of success and hope. IoT helps in managing power consumption of devices and also helps in local savings for user. In modern time, a lot of progress is accomplished with Energy Management System (EMS) and still bettering periodically.
6. Abnormal alarms- With the support of sensors in the devices, abnormal signs of danger such as fire and gas can be monitored. As soon as they are detected, a user is informed of the potential danger through SMS.

3.4 Security in smart home

3.4.1 Security layers

There are said to be six layers in the architecture of IoT - coding layer, application layer, network layer, perception layer, middleware layer, and business layer.

A security network in IoT is commonly divided into three layers namely, network layer, perception layer, and applications layer.

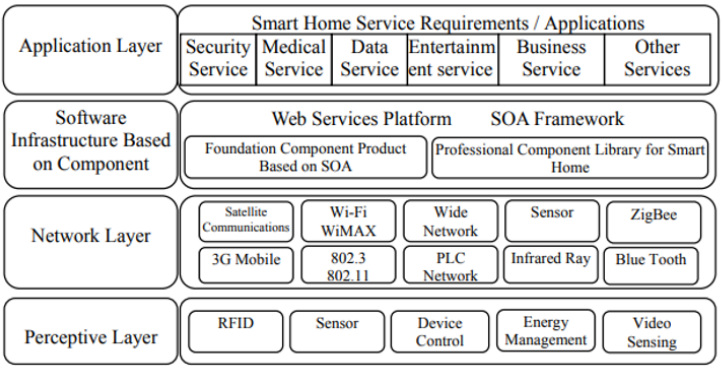

Fig. 3 The architecture of security levels in a smart device[4]

3.4.2 Smart Home Security Objectives

The six most common objectives for smart home security are:

1. Confidentiality: This is a guarantee that the information will be available to the recognized persons only to abstain any misuse of it by any unknown source.
2. Integrity: It protects the data from being tempered by any unauthorized source. A smart gadget can be accessed through a wireless network in such a way that it requires a security system. Effective integrity protects against intentional as well as unintentional alteration, which includes errors and data losses. Hence, hash functions, module codes and digital functions must be used in the files in order to fulfil the purpose.[3]
3. Availability: It assures that the data is accessible to the legitimate user continuously and in timely controlled manner. And if the system is offline, then it should be capable enough to modify the data accordingly. Availability can be secured by limiting certain actions from required functions.[3]
4. Authenticity: It refers to the verification of the identity that is claimed by the user. It can be ensured by verifying the certificate.
5. Authorization: It is again assurance that the access rights of every entity is defined in the system for the control.[3]This term is often used interchangeably with access control or client privilege.
6. Non-repudiation: non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

3.4.3 Security risks

With increasing technology and their popularity, a dangerous environment for malicious actors is served to exploit vulnerable devices from remote places. It is seen in past that any attack on IoT devices can harm millions of devices, as

in Mirai and Hajime cases. Therefore, it brings light on the need to address security issues in IoT.

Security risks will cross over one IoT layer. For instance, the risk of unauthorized access is found for connecting to the main system, the IoT gateway and while logging to the smart home applications. Therefore, a different method is required to identify the user, keeping all these points in mind. Biometric technology is one of the safest and strongest methods for identifying security purposes.

The following figure shows the security risks and its measures in the system at different IoT layers:

Fig. 4 Security risks and its measures in an actual smart home environment [3]

3.4.4 Measures against security problems in smart home

One of the most commonly done mistake in security in IoT devices is the default password. Most of the time users don't change their default password, which makes the gadget an easy attack for DDoS attack.

Secondly, remote access (WAN) of the device should be disabled.

Nowadays, many of the antiviruses also with their signature and techniques helps to curb the growth of the botnet. So, antiviruses should be used in the

system. Moreover, security can be enhanced by using a special username and password on the network.

3.5 Scope for improvement

A smart home is a modest growing technology in the beginning of the 19th century. But it has huge potential in the subsequent time. Their market potential be identified through growth pattern of services in two cases. Firstly, in developed countries such as USA and UK, after a slow take-up in early years there is a significant increase in their adoption overtime. While developing countries according to this pattern may develop the need in future and market can grow. Furthermore, their increased prices in the market, reduces their demands and are currently biggest problem hindering growth of smart homes in developing countries.

According to a report of CISCO, while 500 million appliances were observed in 2003, by 2020 this figure is expected to increase to 50 billion. It can be made more efficient by following ways:

1. Use of webserver- Native applications requires separate versions on different devices. This can be overcome by using a webserver, a single website for all the devices. It is the most open and inoperable way for devices to communicate with each other.
2. Security features- Use of some password or key to access the network, so that risk of the network being infiltered reduces.
3. Independent operation of devices-If smart home devices are operated independently the risk of malicious attacks also decreases, ensuring user's security.
4. User- friendly- user manual button or some interactive guide should be provided for easy control in a developed website interface for users.
5. Automatic functions- The efficiency of the system can be improved by using some automatic functions based on sensors. This will further save time and make the system quick.
6. Solar charger- The use of solar chargers can help in overcoming battery problems. Also, during the blackout, this can act as a backup for device.

4 Conclusion

IoT is bringing a new and revolutionary era in IT industries. It is influencing our lives a lot, from making our jobs easy and efficient to leaking privacy. With its energy management and saving capacity, it can prove to be very useful when energy saving is need of the future. Further, its accessibility and control from a distance are some very useful features. Although user privacy as well as security are big issues, many measures are being taken. With the introduction of more efficient security layers and user passwords in smart home systems, there is a plenty improvement in this matter. With improvement in

some fields and making it more accessible, IoT based smart home appliances can be utilized most effectively.

References

[1] Gunawan, T.S., Yaldi, I.R.H., Kartiwi, M., Ismail, N., Za'bah, N.F., Mansor, H., Nordin, A.N.: Prototype design of smart home system using internet of things. Indonesian Journal of Electrical Engineering and Computer Science **7**(1), 107–115 (2017)

[2] Kadam, R., Mahamuni, P., Parikh, Y.: Smart home system. International Journal of Innovative research in Advanced Engineering (IJIRAE) **2**(1) (2015)

[3] Shouran, Z., Ashari, A., Priyambodo, T.: Internet of things (iot) of smart home: privacy and security. International Journal of Computer Applications **182**(39), 3–8 (2019)

[4] Li, B., Yu, J.: Research and application on the smart home based on component technologies and internet of things. Procedia Engineering **15**, 2087–2092 (2011)