IoT based upon Smart Homes with Security Risk Assessment using OCTAVE Allegro

Research Paper

R Harsharaj

21011101092

AI & DS - B

B.Tech Artificial Intelligence and Data Science
Shiv Nadar University, Chennai

0.1 Introduction

Everywhere we are hearing the word IoT. It simplifies our daily lives where multiple electronic devices which are equipped with a unique IP address and communicated with over internet. In this technology, we can control the number of electronic devices through a single device with the help of the Internet. Here, the electronic devices in IoT technology should have the sensors and it should sense the signal through electrically and functions according to it. And the sensed data transferred to the other device through the Internet. IoT will make our life so simple and accurate. Present this technology has huge job opportunities and still there are many developments are going on. Examples for IoT devices like a smartwatch, smart speakers, smart TV's, Amazon Alexa, Google Home devices are internet-connected devices come under examples of IoT.

Internet of Things has a wide variety of applications and use of IoT is growing so faster. Depending upon different application areas of IoT, it works accordingly as per it has been designed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

IoT can be classified into a four or five-layered architecture which gives you a complete overview of how it works in real life. The various components of the architecture include the following: Four-layered architecture includes media/device layer, network layer, service and application support layer and application layer. Five-layered architecture includes perception layer, network layer, middleware layer, application layer and business layer.

0.1.1 Rise of Iot

The Internet of Things wasn't officially named until 1999, but one of the first examples of an IoT is from the early 1980s, and was a Coca Cola machine, located at the Carnegie Mellon University. Programmers would connect through the Internet to the refrigerated appliance, and check to see if there was a drink available, and if it was cold, before making the trip to purchase one.

Kevin Ashton, MIT's Executive Director of Auto-ID Labs, coined the phrase "Internet of Things" in 1999. He was the first to describe the IoT, while making a presentation for Procter & Gamble, but the definition of the IoT has evolved over time. Mr.Ashton stated:

"Today computers, and, therefore, the Internet, are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a barcode. The problem is, people have limited time, attention, and accuracy. All of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh, or past their best."

The Internet of Things was a common topic used by the media at the beginning of the 21st Century with several major developments paving the way for the future of IoT. LG Electronics introduced the world's first refrigerator connected to the internet in 2000. Allowing consumers to do their food shopping online and make video calls. This invention was followed by a small rabbitshaped robot in 2005 that could report the latest news, weather forecasts and stock market changes. While the first International Conference on Internet of Things was held in 2008 in Switzerland.

In 2012, The Swiss Federal Office of Energy started a pilot program called "Smart City Switzerland." They brought representatives from universities, business, and public administration together to discuss new ideas for the urban environment. Smart City Switzerland has over sixty projects underway and supports new scientific partnerships and innovation.

By the year 2013, the IoT had become a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems. This includes almost anything you can think of, ranging from mobile phones to building maintenance to the jet engine of an airplane. Medical devices, such as a heart monitor implant or a biochip transponder in a farm animal, can transfer data over a network and are members of the IoT.

Today there are more than 27 billion devices connected to the Internet of Things, with experts expecting this number to rise to over 100 billion devices by 2030.

0.1.2 Iot for Smart Home

IoT contraptions are a bit of the greater thought of home robotization, which can fuse lighting, warming and cooling, media and security systems. Long stretch preferences could join essentialness venture reserves by means of ensuring lights and equipment are murdered. Endeavors are pondering and recognizing a huge proportion of IoT-related applications, which can be isolated into two classes.

In first grouping the devices are related, molding an establishment that is mechanized with M2M correspondence and significance to improve people's lives. In this grouping IoT can be seen expecting the activity of TCC&R (track, request and control). In nuclear families for example the room temperature, windows, lights and electrical contraptions, etc would all have the option to be controlled remotely from PC and robotized to discard manual techniques people face step by step in their lives.

For instance, using Apple's Home Kit, producers can have their home things and decoration obliged by an application in iOS devices, for instance, the iPhone and the Apple Watch. This could be a dedicated application or iOS neighborhood applications, for instance, Siri. This can be displayed by virtue of Lenovo's Smart Home Essentials, which is a line of keen home contraptions that are controlled through Apple's Home application or Siri without the necessity for a Wi-Fi interface. The general work in this paper and my examination is to make keen home utilizing web of things with a high security level and including a few gadgets, sensors, controller and so on.

0.1.3 Enabling Technoloogies by IoT

The prevailing improvements in statistics and correspondence advancements (ICT) diagnosed with pc structures, implanted frameworks and guy-made brainpower have made the vision of smart home simply potential. So through enhancing conventional home Automation systems with new first-rate capacities, it's been achievable for sensible domestic circumstance to display one-of-a-kind types of guy-made brainpower. Savvy domestic innovation is the consolidation of innovation and administrations thru domestic structures management for a advanced existence great. The empowering advances for IoT incorporate; Radio Frequency identity (RFID), internet Protocol (IP), digital Product Code (EPC), Barcode, wireless constancy (wireless), Bluetooth, ZigBee, close to Filed verbal exchange (NFC), Actuators, wireless Sensor Networks (WSN) and synthetic Intelligence (AI).

0.2 Architecture

Networked Devices are the physical devices which include sensors, actuators, and transducers. These are the actual devices that collect and send the data for processing. They are capable of receiving real-time data and they can convert the physical quantities into electrical signals which can be sent through a network.

Data Aggregation is a very important stage as it includes converting the raw data collected by sensors into meaningful data which can be used to take actions. It also includes Data Acquisition Systems and Internet Gateways. It converts the Analog signals provided by sensors into digital signals.

Final Analysis is a stage that includes edge IT analytics and the processing of data to make it more efficient and fully capable of execution. It also includes managing and locating all the devices correctly.

Cloud Analysis is where the final data is received here and analysed closely and precisely in data centres. They process and clean the data to make it free from any kind of errors and missing values. After this stage, data is ready to be sent back and executed to perform operations

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five-layer architecture, which additionally includes the processing and business layers. The five layers are perception, transport, processing, application, and business layers. The role of the perception and application layers is the same as the architecture with three layers.

1. The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

2. The processing layer is also known as the middle-ware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.

3. The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

0.2.1 Functions of Each Layer

1. Sensor/Perception layer: This layer comprises of wireless devices, sensors, and radio frequency identification (RFID) tags that are used for collecting and transmitting raw data such as the temperature, moisture, etc. which is passed on to the next layer.

2. Network layer: This layer is largely responsible for routing data to the next layer in the hierarchy with the help of network protocols. It uses wired and wireless technologies for data transmission.

3. Middle-ware layer: This layer comprises of databases that store the information passed on by the lower layers where it performs information processing and uses the results to make further decisions.

4. Service and application support layer: This layer involve business process modeling and execution as well as IoT service monitoring and resolution.

5. Application layer: It consists of application user interface and deals with various applications such as home automation, electronic health monitoring, etc.

6. Business layer: this layer determines the future or further actions required based on the data provided by the lower layers.

0.2.2 Model Design

A essential part of the mission become scheming a version for simulation, checking out and studying effects. AutoCAD was utilized in designing the separate parts of the house version. The layout changed into given as an enter to a laser reduce machine that reduce cardboard to the numerous components of the design. After that, the model turned into assembled to shape the room model supplied in the beneath figures. The parts that were applied within the domestic Automation Simulation are:

- Two RaspberryPi 2 version B: The principle preparing and controlling unit of the framework. One turned into utilized for the room version and the alternative for the reconnaissance automobile.
- Servo Motor: It is going approximately as the entryway lock.
- Infrared (IR) sensor: shows the existing circumstance of the front entryway, both opened or shut.
- Net digital camera: Acts as a reconnaissance digital camera for the room gushing snap shots of that room that are organized by the RaspberryPi. It makes use of OpenCV's picture preparing to have the choice to differentiate questions inside the room.
- Smoke Detector: It identifies hearth, making sure the health of the house.
- H-Bridges: every H-Bridge controls engines, are utilized to control the 4 DC engines of the vehicle.
- Wi-fi Dongle: connected to the Raspberry Pi via USB port to permit its connection to far off web in place of making use of Ethernet link.

0.3 Protocols

Web of Things has various applications in different zones. IoT has been starting at now planned for mechanical WSN. It has been made for Smart Homes System. There are a couple of issues found in IoT and Smart Homes. New advances could help with constraining some of them. This paper presents the issues and challenges that could come. The theory targets were to present the subject of Internet of Things (IoT) and its application to make sharp homes to give getting, comfort and to improve the individual satisfaction. Bringing IoT advancement to our home outcomes in new security challenges, in this manner IoT-based awe inspiring homes require extreme security basics. These moved improvements offer the two prospects and dangers, an IoT-based Smart Home is especially powerless against various security dangers both from inside and outside the home, if security in a shrewd home or astonishing gadget was undercut, and the client's security, solitary data and regardless, success of the occupants will be at risk. Along these lines, sensible assessments must be taken to make the watchful home dynamically secure and appropriate to live in. In any case, we should know precisely what we are trying to ensure about and why before picking unequivocal blueprints. Home Automation is one of the critical usages of IoT. It gives less complex and entertainment living to every person. In this endeavor, a system for working up an IoT programming based canny home computerization structure was completed and attempted through the made model.

0.3.1 Communication Protocols

Some of the Specific IoT Protocols used:

- MQTT : Message Queue Telemetry Transport Protocol
- DDS : Data Distribution Service
- AMQP : Advanced Message Queuing Protocol
- CoAP : Constrained Application Protocol

0.3.2 Zigbee

Zigbee is based on the IEEE 802.15.4 communication protocol standard and is used for personal area networks or PANs. The IEEE 802.15.4 standard has low power MAC and physical layers.

0.3.3 oneM2M

oneM2M brings together all components in the IoT solution stack. It avoids reinvention in favor of reusing existing technology components and standards. oneM2M's architecture defines a common middleware technology in a horizontal layer between devices and communications networks and IoT applications. This standardizes links between connected devices, gateways, communications networks and cloud infrastructure. It allows developers to mix and match components from different vendors.

0.3.4 Z-Wave

The Z-Wave protocol is a wireless, radio frequency (RF) based communications technology designed particularly for control, monitoring and status reading of household applications. Today, over 50 million Z-Wave products have already been sold worldwide. Z-Wave protocol stack contains five layers physical layer, MAC layer, transport layer, network layer, and application layer.

0.4 Conclusion

IoT (Internet of Things) is a network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data. IoT is used to improve efficiency, accuracy, and economic benefit in a variety of industries, such as healthcare, transportation, and manufacturing.

IoT architecture refers to the overall design and structure of an IoT system. It includes the various components that make up the system, such as sensors, gateways, and the cloud, as well as the communication protocols that are used to transfer data between these components. Understanding IoT architecture is crucial for the successful implementation and management of an IoT system.

The technologies supported by IoT are Big Data Analytics, Cloud, Wireless Sensor Networks, Embedded Systems.

Communication protocols are the rules and formats that devices use to communicate with each other over a network. Some common IoT protocols include:

- MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol that is designed for resource-constrained devices and low-bandwidth networks.
- CoAP (Constrained Application Protocol) is a specialized web transfer protocol for use with constrained nodes and networks in the IoT.
- HTTP (Hypertext Transfer Protocol) is the foundation of data communication for the World Wide Web. It is widely used in IoT, but it may not be suitable for all IoT use cases due to its high overhead.

In addition to these specific protocols, there are several standardization efforts underway to ensure that IoT devices can communicate with each other seamlessly, such as oneM2M, Zigbee, and Z-Wave, etc. There are a diverse set of areas in which intelligent applications have been developed. All of these applications are not yet readily available; however, preliminary research indicates the potential of IoT in improving the quality of life in our society. Some uses of IoT applications are in home automation, fitness tracking, health monitoring, environment protection, smart cities, and industrial settings. It is important to note that security is a major concern in IoT systems, as the collection and transmission of data from connected devices can expose sensitive information to potential hackers. Therefore, it's important to consider security measures such as encryption and authentication when designing and implementing an IoT system.