IoT: Review, Security Challenges, Applications

Manjiri U. Karande[1]

[1] *Asstt. Professor, CSE Department, Padm. Dr. V. B. Kolte College of Engineering Malkapur, Maharashtra, India,*

ABSTRACT

The enlarged use of Smart Devices and Mobile Technologies in the different areas has caused great impact on the world. Now days, technology is always changing into some new kind of hardware and software making it obvious for anyone. We are ingoing in a commencement of a new of computing technology known as Internet of Things (IOT). The IoT, refers to the number of physical devices around the world that are now connected to the internet, responsible for collecting and sharing data. The IoT is made up of smart machines interacting and communicating with other machines, environments, objects and infrastructures and the Radio Frequency Identification (RFID) and sensor network technologies. As a result, a very large amount of data is being generated, stored. That data is being processed into useful actions which controls the things or devices to make our lives much easier and secure. Health experts are gradually taking advantage of the benefits these technologies which bring a significant improvement in health care in clinical settings. Similarly, numerous ordinary users are being served from the advantages of the Mobile Health applications and E Health (health care supported by ICT) to improve, help and assist their health. This paper gives an overview of IoT, its applications in various fields, security challenges and opportunities.
Keyword – IoT, RFID, IoT platform, IoT architecture, Security, IoT application

1. INTRODUCTION

The phrase "Internet of Things" was invent by Kevin Ashton in 1999. He made at his place of employment, Proctor & Gamble. During his time there, Ashton came up with the idea to put a RFID tag on each lipstick and let them communicate with a radio receiver. He put forward as fact that such data collection can be used to solve lots of problems in the real world. For most of the current smart household items, we will need to use a different app or website to interface with the device for most of smart household applications. IoT makes this possible due to Ubiquitous Connectivity, widespread adoption of IP– based networking, computing economics, advances in Data Analytics, rise of Cloud Computing hence the IOT is the conjunction of a variety of computing and connectivity trends that have been evolving for many decades [3]. Ubiquitous sensing empowered by wireless sensor Network (WSN) technologies exists many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators [1].

With the continuous advancements in technology a potential innovation, IoT is coming down the road which is flourishing as an ubiquitous global computing network where everyone and everything will be connected to the Internet IoT is continually evolving and is a hot research topic where opportunities are infinite. Imaginations are unlimited which have put it for reshaping the current form of internet into a modified and integrated version. The number of devices availing internet services is increasing every day and having all of them connected by wire or wireless will put a powerful source of information at our fingertips. The concept of enabling interaction between intelligent machines is a cutting-edge technology [2]. There are many IoT applications of innovative concepts such as smart cities, smart/e-health, smart metering and smart things. Each of these applications has particular requirements, i.e., different data rates, low power consumption, low cost of implementation, large number of supported devices and the capacity to cover different distance ranges. appears as a concept that contains both the IoT and the Internet of Humans (IoH), including the capability to share data between each other (IoT and IoH) or among themselves using machine to machine (M2M) or machine to human (M2H) communications [10]. One of the application of IOT is water quality monitoring system. The various issues in this system such as communication, data collection, data analysis, early warnings have been worked on. But in order to get this into picture, technologies and protocols are combined to get the desired output [5]. Five IoT technologies are widely used for the deployment of successful IoT-based products are radio frequency identification (RFID), wireless sensor network (WSN), middleware, cloud computing and IoT application software [6].

2. IOT PLATFORM AND ARCHITECTURE

2.1 IoT Platform

An IoT platform is a multi-layer technology which enables direct provisioning, management, and automation of connected devices within the Internet of Things universe. It mainly connects hardware, however diverse, to the cloud by using flexible connectivity options, enterprise-grade security mechanisms, and broad data processing powers. For developers, an IoT platform provides a set of ready-to-use features which highly speed up development of applications for connected devices as well as take care of scalability and cross-device compatibility. IoT platforms initiated in the form of IoT middleware. Its purpose was to function as a mediator between the hardware and application layers. Its major tasks included data collection from the devices over different protocols and network topologies, remote device configuration and control, device management, and over-the-air firmware updates.
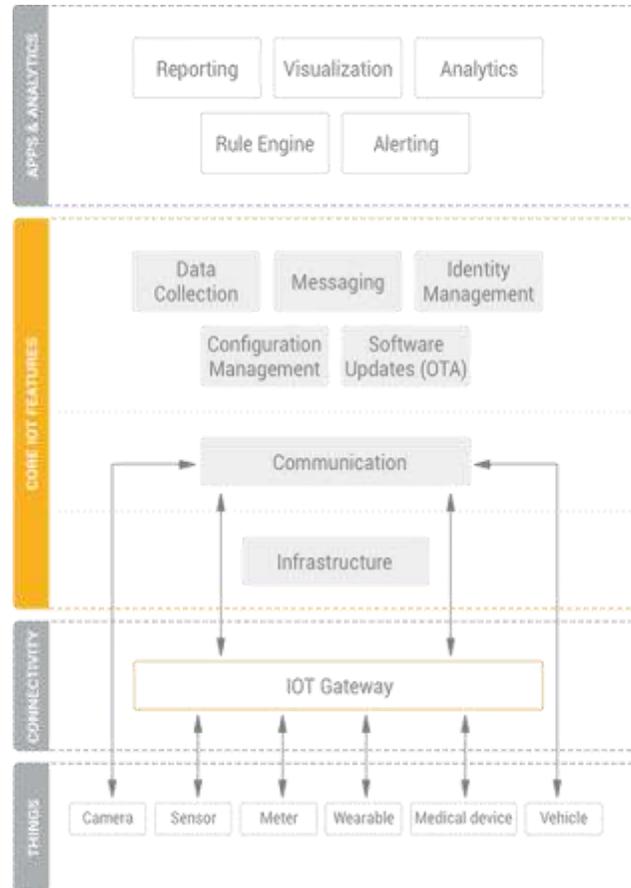

Fig -1 IoT platform Technology stack

A top-of-the-range IoT platform provide you with the majority of IoT functionality needed for developing your connected devices and smart things. The IoT platform stack contains four layers as things, connectivity, core IoT features, and applications & analytics. All the devices connect to the platform, which sits in the cloud or in your on-premises data center, either directly or by using an IoT gateway. A gateway is useful whenever the endpoints are not capable of direct cloud communication

An IoT platform itself can be decomposed into several layers. At the bottom there is the infrastructure level, which is enables the functioning of the platform. The communication layer enables messaging for the devices; in other words, this is where devices connect to the cloud to perform different operations. Among the essential ones are data collection, device management, configuration management, messaging, and software updates.

The top layer is less related to data exchange between devices. But it is useful for processing of this data in the platform. There is reporting, which allows you to generate custom reports. Visualization is useful for data representation in user applications. Then, there are a rule engine, analytics, and alerting to notify you about any irregularities detected in your IoT solution.

2.2 IoT Architecture

For the development of IoT, number of multilayered security architectures are proposed like three-key level architecture of IoT, four-key level architecture. Based on network hierarchical structure six-layerd architecture was proposed which is given in figure 2. The coding layer is base of IoT which provides identification to objects of interest. Each object is assigned a unique ID to easily recognize the object. [2]
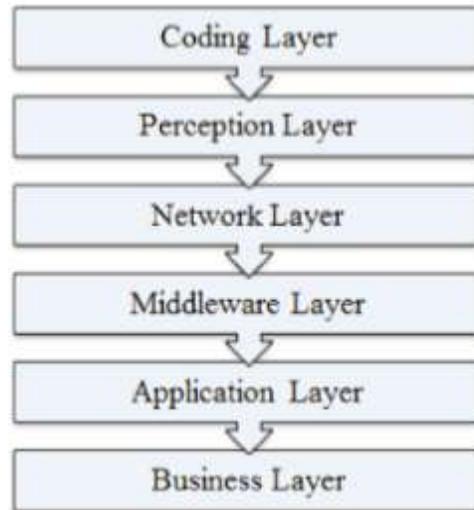

Fig-2 Six-layered IoT Architecture

The next perception layer gives physical meaning to each object. It includes various data sensors like RFID tags, IR sensors which able to sense temperature, speed, humidity, location etc. This layer is perform gathering of useful information of different objects form sensor devices and converts that information into digital signals. These signals are then passed to network layer. Network layer receives these signals and transfer it to middleware layer for processing through Bluetooth, WiFi, Zigbee, GSM, WiMax, with the protocols like IPv4, MQTT, IPv6 etc.[2]

Based on the processed data, the application layer recognizes the application of IoT such as smart homes, smart transportation, smart planet etc. This layer is helpful for development of IoT network widely. The business layer is responsible for the management of the related business under the IoT system.

3. SECURITY CHALLENGES

The latent security threats increases as number and variety of connected devices are introduced into IoT networks. Though the IoT improves the productivity of companies and enhances the quality of living, it also increase the possible attacks surfaces for hackers and other cyber criminals. The study by Hewlett Packard (2014) exposed that most normally used IoT devices contains serious vulnerability and this is due to lack of transport encryption, insecure web interfaces, poor software protection and insufficient authorization. Lack of security will create resistance to implementation of IoT firms and individuals. This can be resolved by training developers to incorporate security solutions like firewalls, Intrusion detection system [6].

In the IoT systems the problem of security and privacy has started to get greater attention from researchers recently. However, the focus of the majority of the publications is on the sensors, networking and application layers in the IoT architecture, quite than the middleware. It is found that only six of the popular IoT including Hydra, GSN, SOCRADES and SMEPP supports security and privacy features. Fremantle and Scott surveyed twenty two IoT middleware systems with the focus on security and privacy. They also found that only ten of the surveyed systems have a security model. Many of them are not well defined and developed. This clearly proves the lack of security support in the existing IoT middleware systems [11].

Authentication and authorization in IoT is an importance research area. Authentication is achieved by methods like ID/ Password, pre- shared secrets, and public key cryptosystem. Authorization can be achieved through data based or crypto based access control. But the rapidly growing number of objects will make the key management system difficult task.

3.1 Privacy in IoT

Now a days, information about user behavior whilst browsing the Internet is collected to enrich the user experience on the Internet. As for IoT, the amount of information collection is not limited to Internet browsing behavior. The information of user's daily routine is also collected so that the "Things" around the user can collaborate to provide better services which fulfill personal preference. Therefore retaining to the collected information which describes a user in detail, conserving the privacy of the collected data is an issue that can be addressed in the case of personal information misusage**.** [12]

3.2 Security protocols and lightweight cryptosystem

Even though various proposed cryptosystems and security protocols are considered secure and robust, they may not be appropriate for the resource-constrained devices in IoT like smart devices, wearable devices, and sensor nodes which have limited battery capacity and computing power.

3.3 Software vulnerability

Software vulnerabilities can lead to a number of backdoor problems. First, with software vulnerabilities, attackers exercise malicious plans without any piece in a victim's system. Accordingly, a backdoor can be planted in a vulnerable device by attackers to control the device. Security mechanisms such as IDS or antivirus that requires fair amount of computation power are not applicable in IoT due to the resource-constraints of IoT devices,. Therefore, it is comparatively easy for attackers to inject backdoor into victim's machine [12].

4. APPLICATIONS OF IOT

4.1 Patient Health monitoring system

Patient Health monitoring system is a reliable and readily available patient monitoring system (PMS). Health is one of the global challenges for humanity The Patient Health monitoring system is used to reduce health care costs by reducing physician office visits, hospitalizations, and diagnostic testing procedure. Many further improvements can be made in this system to make it better and easily adaptable such as adding more advanced sensors. Due to wireless data transmission over internet, health related data will be send to personal computer of doctor or on his mobile. B. N. Karthik et. al.[7] developed system with features like location access, linking the ambulance services, leading doctor's list and their specialist, hospitals and facilities. This system create awareness about diseases and their symptoms through mobile application.

4. 2 In Transportation

Application of the IoT spreads to all aspects of transportation systems including vehicle and driver. IoT in transportation is useful for making a journey from one place to another, and makes it safer and more suitable. IoT plays a key role in all the fields of transportation like water-transportation, air-transportation, and land transportation.[9] Modern automobiles are furnished with sensors which are connected to the internet through control systems. As a result we can say that IoT has vital role in road-safety system such accident detection, traffic signal control, lane changing, etc. [8] The figure shows application of IoT in transportation

Fig-3 Application of IoT in transportation [8]

The vehicle is connected with the several of wireless standards to the internet such as Bluetooth, Wi-Fi, 3G, 4G, intelligent traffic system, and even to other vehicles. IoT in the transportation designed with an advanced form of geo-fencing. It captures the location of device with the coordinates of a specific area. Geofencing assistance in starting the automated tasks. It also allows you to receive a warning when a driver rambles from the suggested path, as it can bring delay in delivery time and cause an accidental loss. [9]

4. 3 IoT in Biometrics

The biometrics security system such as eye scanner system, voice cognition system, and fingerprint system is one of the best applications of IoT. Presently, a biometric system has become a part of everyday life. In most of the company this biometric system works on different parameters like fingerprint sensors, eye scanning system etc. Biometrics uses an individual's physiological and behavioral characteristics like, fingerprint patterns, iris patterns, vein pattern to identify the user. These features are unique to an individual, and also can be used as a secure procedure for authentication [9].

4. 3 Home Automation

Home automation is the housing extension of building automation. It includes the control and automation of lighting, ventilation, air conditioning, heating, and security. Also IoT makes home appliances such as washer/dryers, or refrigerators easily controlling devices. They use Wi-Fi for remote monitoring which are a part of the Internet of things [8]. IoT converts automated home into smart home. With a use of sensors, smart systems, IOT connects everyday objects to a network, which enables those objects to complete tasks and transfer data with each other, with no human input [3].

Table-1 Applications of IoT [4]

Area	Applications
HealthCare/Medical Field	Patient Monitoring, Real-time Health Status
Emergency and Security Area	Global Personnel Monitoring (Location, Health), Resource Planning, Resource Management And Distribution, Detect Explosure And Hazardous Gases, Radiation Level Detection, Liquid Monitor In Data Centers
Supervision of Crowd	Unauthorized And Restricted People Monitoring, Huge Crowd Supervision, Danger Management, Adequate Use Of Public Spaces, Workflow In Commercial Environments
Traffic Management	Smart Transportation Via Real Time Traffic, Path Optimization
Infrastructure Supervision	Sensors Fit Into Infrastructure To Supervise Structural Fatigue, Accident Supervision For Incident Management And Emergency Outcome Coordination
Water Services	Water Quality, Usage, Leekage, Waste Management, Distribution
Building Management Services	Humility Control Management, Temperature, Activity Supervision, Ventilation, Energy Usage Management And Hair Conditioning
Environment	Noise Monitoring, Air Pollution, Industry Monitoring
Smart Cities	Parking Areas Monitoring, Vibrations, Bridges, Material Conditions And Historical Monuments Monitoring, Monitoring In Buildings, Android Devices, Iphone Detection, Energy Radiated Measurement, Traffic Monitoring Vehicle
Smart Agriculture	Soil Moisture Monitoring, Greenhouse Monitoring, Control Humidity And Temperature Levels And Study Weather Conditions
Domestic and Home Automation	Energy And Water Consumption Monitoring, Remote Control Appliances Monitoring, Intrusion Detection Systems, Monitoring Conditions Inside Museums And At Warehouses
Industrial and Control Area	Oxygen Levels And Toxic Gases Monitoring Inside Chemical Plants, Temperature Monitoring, Ozone Level Monitoring

5. CONCLUSION

Each and every object in this world can be connected and take decisions independently with the use of IoT. In today's world IoT makes human life very relaxed with the various applications like health care system, home automation, Road safety etc. This paper describes the layered architecture of IoT. IoT is the network of devices connected to each other through Wi-fi. IoT platform enables the automation and management of devices connected within the IoT. This papers put light on the structure of IoT, security challenges and applications of IoT.

6. REFERENCES

[1]. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "Internet of Thing (IoT): A vision, Architectural elements, and future directions", Future Generation Computer systems 29(2013) 1645-1660.

[2]. M.U. Farooq, Mahammd Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal, "A Review on Internet of Things (IoT)", International Journal of Computer Applications (0975 8887), Volume 113 - No. 1, March 2015.

[3]. Prof.Ms.P.V.Dudhe, Prof.Ms.N.V.Kadam, Prof. R. M. Hushangabade, Prof. M. S. Deshmukh "Internet of Things (IOT): An Overview and its Applications" International Conference on Energy, Communication, Data Analytics and Soft Computing (IMCECDS-2017).

[4]. Akansha Bali, Mohita Raina, Simran Gupta, "STUDY OF VARIOUS APPLICATIONS OF INTERNET OF THINGS (IOT)", lnternational Journal of Computer Engineering & Technology (IJCET)

[5]. Alfiya Abubaker, Kavya C R, Tilju Thomas, Nikhil Joseph, Shifana Begum, "A Study on IOT Approach for Monitoring Water Quality Using MQTT Algorithm", International Research Journal of Engineering and Technology (IRJET).

[6]. In Lee, Kyoochun Lee, "The internet of Things (IoT): Applications, investments, and Challenges for entyerprises", Business Horizon (2015) 58, 431-440

[7]. B. N. Karthik, L. Durga Parameswari, R. Harshini, A. Akshaya,, "Survey on IOT & Arduino Based Patient Health Monitoring System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

[8]. M.Tirupathi Reddy, R. Krishna Mohan, "Applications of IoT: A Study", Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333

[9]. Yusuf Perwej, Kashiful Haq, Firoj Parwej, Mumdouh M Mohammad Hassan, "The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 49, April 2019.

[10]. Victor Baños-Gonzalez, M. Shahwaiz Afaqui, Elena Lopez-Aguilera and Eduard Garcia-Villegas, "IEEE 802.11ah: A Technology to Face the IoT Challenge", Sensors 2016, 16, 1960; doi:10.3390/s16111960.

[11] Anne H. H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng, Member, IEEE, "IoT Middleware: A Survey on Issues and Enabling Technologies", IEEE INTERNET OF THINGS JOURNAL, VOL. X, NO. X, MARCH 2016.

[12] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, IEEE Fellow, "IoT Security: Ongoing Challenges and Research Opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications.