The Study of Layers and Security Issues in IoT for Home Automation Applications

Dr. G. Rama Subba Reddy
Associate Professor,Dept. of CSE
Mother Theresa Institute of Engineering & Technology
Palamaner, Andhra Pradesh

Dr. S.Murali Mohan
Professor,Dept. of ECE
Mother Theresa Institute of Engineering & Technology
Palamaner, Andhra Pradesh

Dr. M.Lakshimikantha Reddy
Principal, Mother Theresa Institute of Engineering & Technology
Palamaner, Andhra Pradesh

Abstract

The era of computing concentrates on meeting the goals of automation through the enhancements in technical aspects by Internet of Things (IoT). IoT refers to a wireless network of various interconnected components and is pervasive in our day by day life. Standing out from customary web, IoT won't utilize the assistance of human for completing a particular work. These gadgets can sense the data, and process it using automated tools and these data can be utilized by any real time applications now a days. At the end of the day, some meaningful information can be extracted from these sensor data and used by converting in to human or computer recognized format. The uses of IoT, incorporate smart homes, forest monitoring, health monitoring and numerous data science applications. Nonetheless, using the same has drawbacks on providing the privacy and security of the data and designing new strategies for improving the securityis prior to any filed. In this paper, we presented the brief review on providing the security and protection and every layer in the IoT architectures along with some research gaps in the literature. The commitments of this paper incorporate, the basic elements in IoT and numerous applications of IoT along with some issues, challenges faced in smart homes.Another major problem of IoT is the batter power and needed evolutionary techniques to improve the methods, how to Extracting the useful information from the sensor data when the battery is dead.

Keywords – IoT elements, data abstraction, architecture, security and protection.

1. Introduction

The era of computing concentrates on meeting the peaks of automation through the enhancements in technical aspects by Internet of Things (IoT) which refers to a wireless network of various interconnected components. Those interconnected components interact with each other even though there is no human involvement. It happens whenever our environment wants to be embedded with sensors and other technologies such as Radio Frequency Identification (RFID), Wireless Sensor Network (WSN) etc., help to overcome this issue. Kevin Ashton was the first person who proposed IoT in 1999 beyond the supply chain management. As stated in GSMA, IoT refers to the usage of logically connected components and also the systems for supporting the collected data via fixed sensors together with the actuators in the machinery and as well as other physical components[1]. The collected information needs huge space to store the outcomes in its reliability over cloud computing. The part of IoT is called as Machine to Machine (M2M) interaction which is already using wireless networks to connect the devices with each other through internet where there is less involvement of human.

The devices of IoT are equipped with sensors and the processing power which enables them to constitute in various environments. Figure 1 depicts various usual applications of IoT where there includes a smart home/city, smart clusters, medical and as well as healthcare providing, and so on. This paper provides a simple introduction to the IoT, its application and potential benefits to the society. We are going to cover the applications of IoT in further level in section 2.1. The fast growth in the count of used IoT devices would reach 50 billion by the year 2020, which stated in the report of International Data Corporation. Only one difference between IoT and the traditional internet is that there will be no human involvement in both. IoT has received much attention from scientists, industry and government all over the world for its potential in changing modern day living. IoT is envisioned as billions of sensors connected to the internet through wireless and other communication technologies. The sensors would generate large amount of data which needs to be analyzed, interpreted and utilized [2]. Home Automation System uses the technology of Internet of Things for monitoring and controlling of the electrical and electronic appliances at home from any remote location by simply using a Smartphone. Implementation of a low cost, flexible home automation system is presented. It enhances the use of wireless communication which provides the user with remote control of various electronic and electrical appliances. This paper presents basic information about IoT, applications of IoT and possible advantages to society [1]. IoT got high attention from the researchers, industries and government at global level. In IoT, the sensors will create huge data that requires analysis, interpretation and usage [2]. The home automation system utilizes the IoT technology to monitor and control both electrical and electronic devices at home from any remote places simply by the use of smartphone. The implementation will be done on low cost and flexible home automation system is presented. It increases the usage of wireless interaction which enables user to control many electronic and electrical components remotely [4].

2. Related Work

In this section, we presented one application of IoT i.e. Home Automation along with few research gaps. A key factor is to be considered in the case of home automation is that is Security. The most important feature and also very crucial in home automation is Home security. This home security made many changes in the last few years and proceed to improve more in upcoming years. There exists some technologies, in which the user can control all the things by operating remotely with their smart phone. With those smart phones the owner can also control the alarm like to stop or to start remotely. This scheme helps the users to protect their homes. There was unequalled growth in number of gadgets being connected to Internet since past few decades and are considered as a part of an IoT infrastructure and can send and receive the data among each other. So that it is an advantage for using such prevailing infrastructure to model the recommended security system. The proposed system always keeps owner get informed about the status of his home security and so that he can take corrective actions.

Govinda et al (2014) discussed about the designing and implementing of Security to a smart home on the GSM technology basis which allows two schemes for the implementation of home security by using IoT [5]. The first one is whenever any motion is identified by a camera then it makes an alarm sound and notifies a mail to owner. For this the cameras must have good quality i.e. should have extensive range and image quality must be good enough to find the movement. Karri and Daniel (2005) proposed SMS oriented system that uses GSM to utilize internet services for sending messages or notify house owner instead of sending SMS. [6]. Jayashri and Arvind (2013) was applied a fingerprint based authentication scheme to unlock the door [7]. This system helps the users to have an access whose fingerprint are authorized by the owner of the house. This system includes some more features to protect home like gas leakage and in the time of fire accidents. Some of the experts argued that depending only on fingerprint system is not always good one because it is easy to replicate someone’s fingerprint so instead this fingerprint scanners with the extra layer of security is now available like PIN , passcode, voice recognition and so on are advised to use. Few researchers suggested a notion for keeping IoT home security system robust where a fault in one device in the system does not influence the working of entire system [8].

Besides, the scheme has ability to utilize overlap between many gadgets which results in energy preservation so that to make high efficient model. For the model we stated earlier is provided an instance model which uses temperature sensor, Wi-Fi module and a door sensor to replace a fault camera. Laser rays and LDR sensors are utilized to find intrusion based on their movement was introduced in 2016 [9]. The way the system process is that a laser is focused towards a LDR sensor and the moment that the contact of laser to LDR sensor breaks, the alarm is connected to the sensor goes off alerting the neighbors and sends a SMS to the owner. This system overcomes the issue of capturing the places those are not in range from the installed cameras but faces the similar obstacles that raises with the systems having GSM modules for sending SMS. The message delivery depends on the network coverage. Besides the lasers has straight beam, so that intruders who knows about system can easily dodge the lasers and make the total system not to work. The new way to model an electronic lock is by using Morse code and IoT technology [10]. The authors declare that it is a genuine notion not anyone tried it before and it is first of its type “optical Morse code-based electronic locking system”. This system utilizes LED’s (Light emitting diodes) as an encryption medium for sending signals. At the receiver’s side is a photosensitive resistor as well as microcontroller like an Arduino processor that is capable of decrypting the optical signal when it receives them from a LED. The researchers done research n system in a real time and was proven that they are intended to work in various illumination environments with completely working functions. They also declare to have an interface which is easy and also user-friendly. Anitha et al (2016) introduced a home automation system using an artificial intelligence and also suggested a model for the cyber security systems [11].

2.1 Applications of IoT

Numerous application domains which get impact by the rise of IoT. Those applications are classified on the basis of availability of type of a network, coverage, scale, heterogeneity, replication, human involvement and their impact. IoT permits the every industry’s organization to offer the innovative services and update their business strategies. We mentioned few of the application areas here. The first application of IoT is using in **Smart Applications and Smart cities.** IoT has its key application in smart home environments, where there is having various devices that enables the automation of general internal activities. Several applications which are related to a smart home environment recommended in literature involved (wireless) sensors networks. IoT can provide general middleware for the future based smart city services collecting information from different sensing infrastructure attaining total kinds of geo-location and also IoT technologies. Many recently recommended solutions suggest to use the Cloud architectures to permit the identification, connection and integration of sensors along with the actuators, so making platforms so that to supply and support frequent connectivity and real-time applications for smart cities.

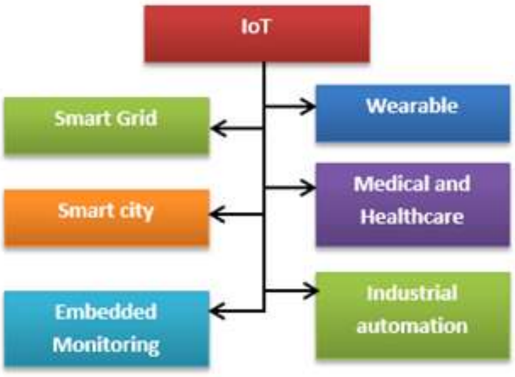


Figure 1: Applications of IoT

Smart devices, mobile internet and cloud services give the continuity and framed identification of **healthcare** and permits the cost effective, efficient, timely basis and high quality of medical services. Those services whichever provides will include the management of different chronic diseases, adult care, fitness activities and so on.In the field of **utilities** IoT application has actual time collection of utilized data, local balancing, demand and supply forecasting, runtime tariff generation and so on; users connected to such smart networks was with the significant cost and resource savings. In **manufacturing**, some of the solutions suggested by IoT are equipment handling and diagnostics through sensors which are placed on production floor, remote monitoring and diagnostics, automation of production lines and so on. The result ranges from optimized field support costs, minimizes the breakdowns to greater operational efficiency.Due to technological enhancements, IoT is seeking to provide challenging ways to change the transportation systems along with the **automobile services** (i.e. Intelligent Transportation Systems, ITS). The recent generation of IoT based vehicular data; Clouds could be developed and are provided to balance many business benefits, such as improving the road safety, optimizing traffic congestion and its management as well and assisting maintenance of car. Though, there are some technological advancements in IoT in meantime the applications which are achievable are outlined in above may be quite interesting. In addition to this, one prediction is to make the technology available with low costs, if more objects are essentially to be equipped. Along with this we faced many other challenges like scalability, Discovery, Flexibility, Interoperability, Integration of data from multiple sources, Security, Power supply, Energy Efficient Sensing, Fault tolerance and privacy. The future of IoT includes the following elements.

2.2 Quality of Service

In Cloud computing, another key research field is QoS which needs more attention as the data and instruments are having access on clouds. Dynamic scheduling and algorithms related to resource allocation on the basis of particle swam optimization are generated. The first one is deriving **new protocols.** The protocol at the end of IoT plays an important role in entire realization. They make a support to data tunnel between the sensors and also external environment. For efficient processing of a system mainly it requires an energy efficient MAC protocol and applicable routing protocol. Second, Modern visual technologies emerge, innovative **visualization** is allowed. The enhancement from CRT to Plasma, LCD and LED assist to more efficient data representation (using touch interface) with the user and is able to cover the data better than ever. At last, the combined applications of **IoT and Cloud computing** enables the creation of smart environments such as smart cities and are able to include the services offered by many stake holders and evaluate to support many more users in decentralized way with good reliability.A Security Framework for the Internet of Things in the Future Internet Architecture and is shown in Figure 2. The Mobility First-based IoT architecture comprises of four basic building blocks: Devices, IoT middleware, Mobility First network and Applications. Our aim is to provide clear and safe data to several applications/services in the upper layer and make their development/management easier.

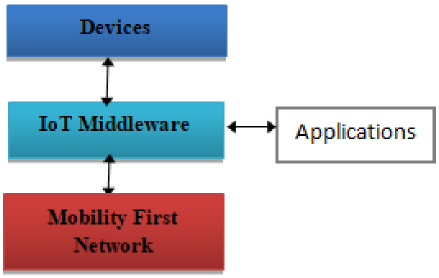


Figure 2: IoT middleware and Mobility First network.

2.3 Abstraction

In this section, we have discussed about the terms data abstraction upon sensor data and its different representation ways includes with multiple levels of abstraction, its variations with the other research domains and also discussed about motivation and challenges in creating abstractions on the basis of sensor information.In IoT the label abstraction was coined in sense of computing domain, describing various levels transformation incorporated from the sensing layer to a perception layer. Such process of transformation was proposed by Chen and Kotz [12] as defining the top level context data from low level context sensor data via collecting, aggregating and inferring of raw data with additional knowledge by environment with the perception of adjusting the sensor devices behavior to the recent context. The aim of dual granularity abstraction levels to represent the intelligence with the user-centric focus, first one is lower level abstraction (or data abstraction) and the other one is higher level abstraction (or semantic abstraction). A lower level abstraction represents the atomic and static information which is achieved by data collection from user local sensor information and by including that information with Meta data upon local sensors such as its type, range and abilities. The motivation for the data abstraction is that, there is high demand for recent data processing techniques and concepts to work with the big data issues. We contribute data abstraction which can be used to reduce information. Focusing on the abstracted information rather than numerical information will have two important advantages one is optimization of network traffic and second is the enhancement of comprehensiveness to the end-user. Data abstraction is utilized as a basis for prevailing techniques such as outlier detection, activity recognition, and other emerging areas in sensor networks domain.

3. Limitations of IoT Devices

There are two key restrictions on the generic IoT technologies. One is battery capacity and the other is computing power.

3.1 Battery Life Extension

Some of the IoT gadgets are kept in the places where there is no chance for charging. Three strategies are possible to overcome the problem of charging availability. The first is to use few security essentials on a device which is not assisted especially during its work with sensible data. The second strategy is to increase the battery capacity. The final one is energy saving from the natural resources like light, wind, heat and vibration.

3.2 Lightweight computation

In [9] paper it states that conventional cryptography which do not work with IoT systems since the gadgets are having limited memory space and therefore it is not able to handle the computing and storage requirements of advanced cryptographic models. The researchers suggested that to reuse the existing functions for giving support for security mechanism of limited gadgets. For example utilization of physical layer authentication via applying signal processing at receiver side is to check whether the transmission is done from the desired place. On other side, the features of special analog transmitter are effectively used to encode data. The authors in [13] proposed a paradigm of encrypted query processing for IoT. This technique allows for storing the encrypted IoT data safely upon cloud, and supports for efficient database query processing on encrypted data. In [14] the researchers proposed a method to reduce IoT latency during query processing on encrypted data by the application of latency hiding approach which comprises of break down query outputs of big size to small sized data sets.In [15] the authors recommended a light weight encryption technique for smart homes on the basis of Identity-Based Encryption (IBE) where the public keys are simply identity strings with no need of digital certificate.

4. Security

Applying the existing internet standards to smart devices becomes easier to integrate the intended IoT context scenarios. Besides the security based mechanisms in conventional Internet protocols need to be changed or elaborated so that to support IoT applications. Here we have discussed the security related issues and available solutions in various layers in IoT systems and is shown in below Figure 3.Here, Layer 1 is the bottom layer and is so called as the things layer. It comprises of devices, sensors, controllers etc. The next layer is a Connectivity/Edge computing layer which defines different communication protocols and networks utilized for connectivity and also for edge computing. Layer 3 is a Global infrastructure layer. This layer is typically implemented in the cloud infrastructures. Layer 4 and Layer 5 are related to a Data ingestion and data analysis. It includes big data, cleansing, streaming and storage of data. Then layer 5 relates to data reporting, mining, machine learning and so on.Application layer comprises of custom applications which actually make use of the things data. There is also a layer called a People and Process layer which it includes with people, businesses, collaboration and decision making depending on the data derived from an IoT computing.

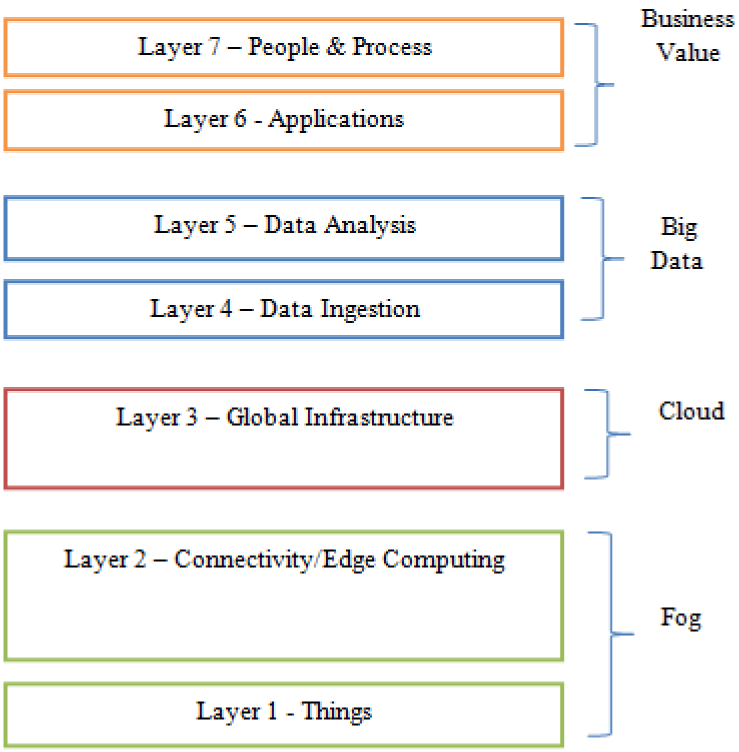


Figure 3: Security at each Layer

IoT Perception Layer

The development of IoT is specialized for collecting and exchanging the data in physical world. Hence the perception layer comprises different types of collecting and managing the modules such as temperature sensors, noise sensors, vibration sensors and so on. This layer is again divided into two parts: a perception node (sensors or controllers and so on), a perception network which interacts with a transportation network [16]. A Perception layer technology includes with WSNs, Implantable Medical Devices (IMDs), radio-frequency identification, global positioning system etc. To meet the service quality, it is necessary to identify the false nodes and correct actions are to be taken in order to neglect the immediate service degradation. Wang et al. [17] was derived the intrusion detection probability in the both homogeneous and heterogeneous WSN.

IoT Network Layer Security

In WSN context, the IoT devices require to extend the IPV6 on powerless wireless PANs (6LoWPAN) to permit an IPSec communication with IPv6 nodes. It is advantageous as the existing end-points in Internet are required to change and interact with WSN securely and the actual E2E security is implemented with no trustworthy gateway. Raza et al. [18] proposed an E2E secure interaction between an IP enabled sensor networks and their extension to LoWPAN supports with the both IPSec's authentication header and also Encapsulation Security Payload (ESP), hence the end-points of communication get authenticate, encrypt and evaluate the integrity of message by the utilization of standardized and established IPv6 mechanisms.

IoT Transport Layer Security

Kothmayr et al. [19] introduced the first totally implemented a two-way authentication strategy to IoT system based on existing internet standards, particularly DTLS protocol. The proposed security method is implemented during totally authenticated DTLS handshake and relying on exchanging of the X.509 certificates which is having RSA keys. They connected with a compressed DTLS with 6LoWPAN standard by utilizing standardized mechanisms.

IoT Application Layer Security

IoT has extensive range of applications but not only limited to smart home (e.g., learning thermostat, smart bulb) and it also includes with medical and healthcare (e.g., real-time health monitoring system), smart city (e.g., smart lighting, smart parking), energy management (e.g., smart grids, smart metering), environmental monitoring (e.g., climate monitoring, wildlife tracking), industrial Internet, and connected vehicle. Most of the recent IoT gadgets consist of configurable embedded systems. When we connect those to internet they can get infected by computer virus like Trojan [20].

5. Elements of IoT

In this section, we are going to discuss about the architecture along with its basic elements. In broad, IoT architecture contains three layers such as application, network and perception layer. There are mainly six key elements that are essential to allow the functionality of IoT. These six elements i.e. Identification, communication, sensing, computation, services and semantics are further classified as shown in Table 1, we have also shown an example for each.

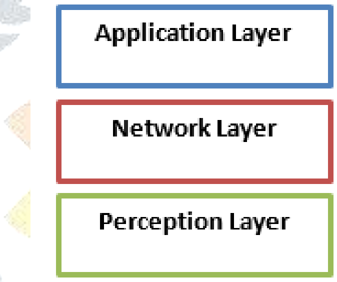
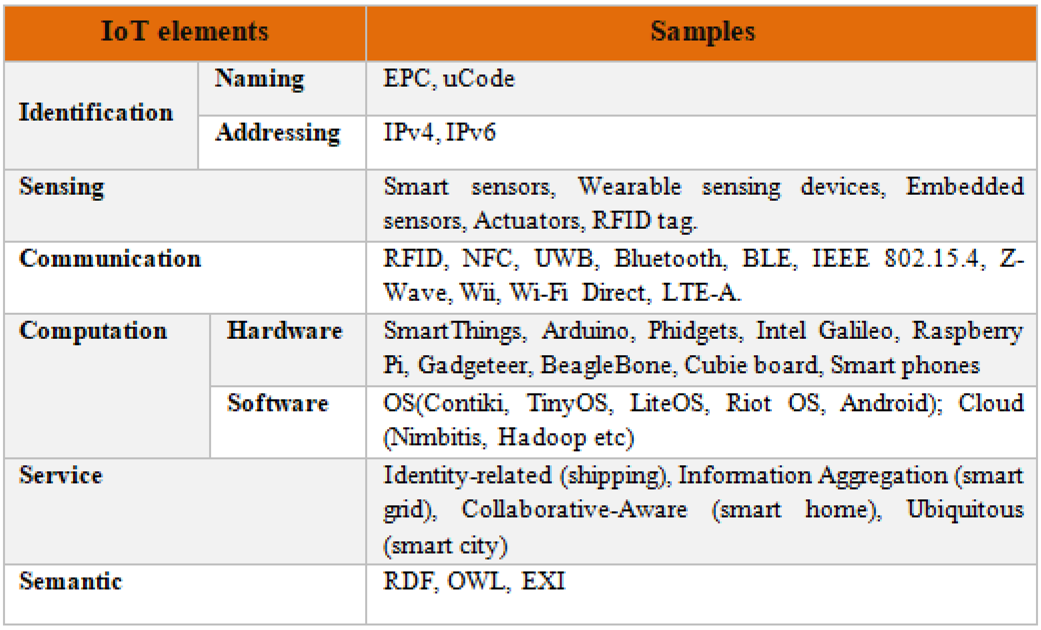


Figure 4: IoT Architecture

Identification plays an important role in IoT to provide identity and connect the services relying on its demand. There are various methods for IoT such as Electronic Product Codes (EPC) and Ubiquitous Codes (uCode) [21]. Besides it is hard to address the objects of IoT while separation between an object ID and its address. An object ID represented its name as “T1” for particular temperature sensors and object’s address represents its self-address in a communication network. Additionally IoT addressing approaches includes IPv6 and IPv4. 6LoWPAN [22] enables optimization technique over IPv6 headers that makes IPv6 addressing as related to low power wireless networks. Identification schemes are used to provide a clear identity to every object in the network.**Sensing** refers to data collection from the related objects of internal network and sending it back to a data warehouse, DB or a cloud. We must analyze the collected data to specific actions based on required services. The IoT sensors may be sensors, wearable sensing devices or actuators. For instance, few companies like WeMo, Revoly and Smart Things allows smart hubs and also mobile applications that enables people will monitor and handle smart gadgets and home appliances using their smartphones [23].



IoT elements		Samples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag.
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, Wii, Wi-Fi Direct, LTE-A.
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubie board, Smart phones
	Software	OS(Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbitis, Hadoop etc)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

Table 1: IoT elements

The **communication** based technologies in IoT will connect different kinds of objects together to deliver particular services. Generally the IoT nodes need to be operated through the utilization of low power in the presence of noisy and lost communication links. Few of communication protocols utilized for IoT are WiFi, Bluetooth, IEEE 802.15.4, Z-wave and LTE-Advanced. Some of the communication technologies especially like RFID, Near Field Communication (NFC) and ultra-wide bandwidth (UWB) are in use. RFID is the first technology which is used to realize M2M concept (RFID tag and reader) [24]. Several hardware platforms are developed to run some of the IoT applications like Arduino, UDOO, Intel Galileo, Beagle Bone, Wi Sense, Friendly ARM, Gadgeteer, Z1, Raspberry PI, Cubieboard, Mulle and T-MoteSky [25].

The **semantics** in IoT refers to the capability of achieving knowledge easily by various machines to provide the required services. Extraction of knowledge includes detecting and utilizing the resources and as well as data modeling. Additionally it also includes finding and analyzing data for better decision making to give actual service. In 2011, the World Wide Web consortium (W3C) adopted the Efficient XML Interchange (EXI) format as a recommendation [26].To understand the vision of IoT is hard since various challenges are to be stated. Some of the major challenges are its availability, mobility scalability, security, trust, reliability, performance, interoperability, security and management. Intimating those challenges enables service providers and also application programmers for their services applying very efficiently.

Along with security and privacy there are other quality evaluation metrics include Availability, Reliability, Mobility, Performance, scalability, interoperability affect the outcomes of IoT applications. **Availability** is to be done in both hardware and software levels to provide services at anytime and anywhere to customers. **Reliability**refers the systematic processing of a system depending on its specification. The aim of it is to increase the success rate in providing the IoT services. Another challenge in IoT applications is **Mobility**. Since there is need to deliver more services to the mobile users. The obstacles while the delivery of services to mobile gadgets happens when such gadgets moves from one gateway to the other. [27] Introduce a resource mobility strategy which permits dual modes such as caching and the other is tunneling for encouraging the continuity of services.**Performance e**stimates the IoT services and its performances is a big challenge as it depends on the performance of various components. Similar to the other systems, an IoT needs developing and improving its services to attain the requirements of customer's. The **Scalability** of IoT refers to the capability of including new devices, services and its functions to users without having any negative impact upon the quality of existing services. Adding new functions and recommending new devices is not an easy task especially in the sense of several platforms and also communication protocols.Another IoT challenge is that End-to-end **interoperability** to manage different kinds of objects related to various platforms. Interoperability need to be compared with the both application developers and manufactures of IoT gadgets to accomplish the transfer of services for all users in spite of their using requirements related to hardware platform. For example, in today's many smart mobiles supports basic communication technologies such as Wi-Fi, NFC and GSM to satisfy interoperability in different scenarios.

6. Conclusion

IoT is a system of connected components where there is a possibility of converting a normal device to a smart device. Besides there is a capability to transfer the data in a network even in the absence of human. Among the applications of IoT, Home automation is having a significance since the entire world is going towards the smart world. In this paper we described about the significance of home automation and related works on it. Additionally we also presented the applications, challenges and future of IoT. A security based framework for IoT is being explained here and as our motto to provide clear and secure data to users. The security based issues at multiple levels of IoT architecture are discussed. Under information abstract section we have discussed regarding data abstraction on sensor information and its different ways of representations and its variations with the other research fields. We also addressed the limitations of the computing gadgets like battery power and computing capacity along with the basic elements of IoT.

REFERENCES

[1] Understanding the Internet of Things (IoT), GSMA Connected Living

[2] What the Internet of Things needs to become a reality, White Paper, Global Strategy and Business Development, Freescale and Emerging Technologies, ARM.

[3] J. Coutaz, J. L. Crowley, S. Dobson, and D. Garlan, "Context is key," Commun. ACM, vol. 48, no. 3, pp. 49–53, 2005.

[4] S.M.RiazulIslam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, Kyung-SupKwak, "The Internet of Things for Health Care: A comprehensive Survey", IEEE Journal Vol.3 2015.

[5] Govinda K and Sai Krishna Prasad K and Sai ram susheel 2014 Intrusion detection system for smart home using laser rays International Journal for Scientific Research & Development (IJSRD) 2 176-78

[6] Karri V and Daniel Lim J S 2005 Method and Device to Communicate via SMS after a Security Intrusion 1st International Conf. on Sensing Technology Palmerston North New Zealand 21-23

[7] Jayashri B and Arvind S 2013 Design and Implementation of Security for Smart Home based on GSM technology International Journal of Smart Home 7 201-08

[8] S. Raza et al., "Securing communication in 6LoWPAN with compressed IPsec," in Proc. Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSS), Barcelona, Spain, Jun. 2011, pp. 1–8.

[9] Cristian C, Ursache A, Popa D O and Florin Pop 2016 Energy efficiency and robustness for IoT: building a smart home security system Faculty of Automatic Control and Computers University Politehnica of Bucharest, Bucharest, Romania 43

[10] Lee C T, Shen T C, Lee W D and Weng K W 2016 A novel electronic lock using optical Morse code based on the Internet of Things Proceedings of the IEEE International Conference on Advanced Materials for Science and Engineering eds. Meen, Prior & Lam

[11] Anitha A, Paul G and Kumari S 2016 A Cyber defence using Artificial Intelligence International Journal of Pharmacy and Technology 8 25352-57

[12] G. Chen and D. Kotz, "Context aggregation and dissemination in ubiquitous computing systems," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 105–114

[13] S. Raza, S. Duquennoy, J. Hoglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—A comparison of link-layer security and IPsec for 6LoWPAN," Security Commun. Netw., vol. 7, no. 12, pp. 2654–2668, 2014.

[14] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Netw., vol. 11, no. 8, pp. 2710–2723, Nov. 2013.

[15] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN compressed DTLS for CoAP," in Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst., Hangzhou, China, May 2012, pp. 287–289.

[16] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," Wireless Netw., vol. 20, no. 8, pp. 2481–2501, 2014.

[17] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Trans. Mobile Comput., vol. 7, no. 6, pp. 698–711, Jun. 2008.

[18] S. Raza et al., "Securing communication in 6LoWPAN with compressed IPsec," in Proc. Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSS), Barcelona, Spain, Jun. 2011, pp. 1–8.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Netw., vol. 11, no. 8, pp. 2710–2723, Nov. 2013.

[20]. Yuchen Yang et.al. "A Survey on Security and Privacy Issues in Internet-of-Things", IEEE Internet of Things Journal Vol 4, No. 5, October 2017.

[21] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitous computing and the Internet of Things," IEEE Pervasive Comput., vol. 9, no. 4, pp. 98–101, Oct.–Dec. 2010.

[22] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," Internet Eng. Task Force (IETF), Fremont, CA, USA, Internet Proposed Std. RFC 4944, 2007.

[23] U. Rushden, Belkin Brings Your Home to Your Fingertips With WeMo Home Automation System. Los Angeles, CA, USA: Press Room Belkin, 2012.

[24] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," IEEE Wireless Commun., vol. 12, no. 1, pp. 12–26, Feb. 2005.

[25] A.Dunkels,B.Gronvall, andT.Voigt, "Contiki—A light weight and flexible operating system for tiny networked sensors," in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., 2004, pp. 455–462.

[26] T. Kamiya and J. Schneider, "Efficient XML Interchange (EXI) Format 1.0," World Wide Web Consortium, Cambridge, MA, USA, Recommend. REC-Exi-20110310, 2011.

[27] F. Ganz, R. Li, P. Barnaghi, and H. Harai, "A resource mobility scheme for service-continuity inthe Internet ofThings,"in Proc.IEEEInt. Conf. GreenCom, 2012, pp. 261–264.

Author's Biography:

Dr. G. RamaSubba Reddy received his Ph.D in Computer science & Engineering from Sunrise University. He received his M.E in Computer Science & Engineering from Sathyabama University, Chennai. Presently he is working as an Associate Professor and Head of the Department in Computer Science & Engineering, Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh. His current research focus is on IoT, Data mining and Cloud computing.

Dr. S. Murali Mohan received his Ph.D in Electronics & Communication Engineering from S. V. University. He completed M. Tech in VLSI Design from BIHER and B. Tech form Bangalore University. Presently he is working as Professor and Head of the Dept. of ECE, Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh. His current research focus is on IoT, Neural Networks and VLSI Design.

Dr. M. Lakshimikantha Reddy received his Ph.D in Mechanical Engineering from JNTUA, Ananthapuram. He received M. Tech from IIT Madras. Presently he is working as Principal, Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh, with the vast experience of twenty two years in various positions.