A Literature Study on Issues, Challenges, Limitations of Internet of Things

B. Mounika[1], B. Mamatha[2]
[12]Assistant Professor, Department of CSE
[1] AITS, Rajampet, A.P, India
[2] KLM College of Engineering for Women - Kadapa, A.P, India

Abstract- Internet of Things (IoT) is ubiquitous in our daily life. Contrasting with traditional internet, IoT will not use the help of human for doing a specific task. These devices can capture the data, analyze, and process itself. In simple words, IoT refers to the interaction and the communication between millions of hardware devices, which produce and transfer data automatically related to the real world objects i.e. things. Retrieving the high level content from the low level sensor data has wide range of applications. In other words, meaningful abstractions are collected from the raw data and this will be presented in to the human or machine understandable format. The applications of IoT, include online health monitoring, environmental monitoring, smart home applications etc. However, if we used IoT in any field there will be a big risk of content or data privacy along with some security issues. It is essential to design and implement efficient methods and machine learning models for extracting the useful content from the raw data as well as for representing the data and patterns visually easier to the users. At the same time we need to manage the privacy and security of these information. Many studies are done to provide the secure IoT devices and provided good measures to reduce such kinds of risks. We presented a brief study on the privacy and security in each layer of the IoT architecture. The contributions of this paper includes, study of IoT i.e. the applications and the research gaps exist in the literature and also included the current challenges in this field. Additionally, the information abstraction and the work flow for mining useful information from the input or sensor data.

Keywords- *IoT, abstraction, security, layers, IoT elements*

I. INTRODUCTION

The epoch of computing focus on reaching the heights of automation via the technological advancements by IoT (Internet of Things). IoT is the wireless network of several interconnected gadgets (devices/things) that interact with each other in the absence of human. This occurs when our environment want to embed with the sensors and technologies like RFID (Radio Frequency Identification), WSN (Wireless Sensor Network) and so on enable us to overcome this challenge. IoT was firstly introduced by Kevin Ashton in 1999 in the backdrop of the supply chain management. However the definition of the things was modified as the technology evolved. According to GSMA, the IoT refers to the utilization of logically connected things and the systems to support gathered information by fixed sensors along with actuators in machinery and other physical devices [1]. The gathered data requires more space for storage results in its reliability upon cloud computing. A portion of IoT is known for Machine to Machine (M2M) interaction that already used wireless networks for connecting devices with each other via internet with less intervention of human. The innovation of this period is limitless with surprising potential to enhance our living standards.

The IoT gadgets are provided with the sensors and the power of processing that allow them to establish in different environments. Figure 1 constitutes several usual IoT applications that includes with smart home, a smart city, smart clusters, medical and healthcare furnishings, connected vehicles and so on. The rapid increment in the count of the utilized IoT gadgets may reach 50 billion in 2020 with $9 trillion market [23] as specified in the report of International Data Corporation of 2013. The only difference between an IoT and the conventional Internet is that there is no presence of Human. The IoT devices are able to generate data regarding one's behaviors, analyze that data and also take action [24].

In current days IoT is everywhere such as at railway stations, shopping malls, at colleges an information desk became mandatory to provide information regarding train schedule, promotional offers and for getting notifications immediately in many other applications. From an educational instutional's perspective, the issue is that it need some staff and that should have recent information upon the institute and also the earlier happenings in that institute. Another issue is that a person has to go the institute at this information desk to retrieve information through them. The solution for this issue is we have to use technology and make that technology responsible to clear all the queries of people. The best instrument is mobiles, since they are available for everyone and it must be connectable to the internet in order to download the recent information. If that information is not updated on the internet, in that case we have to call customer service center for support.

II. APPLICATIONS & FUTURE

There exist numerous application fields which get influenced by arising of IoT. The applications might be categorized on the basis of availability of network type, its coverage, scale, heterogeneity, repeatability, involvement of user and their influence [2]. IoT allow the organization of every industry for providing the innovative services or modify their business methods. Few of the applications are described below.

Smart Applications and Smart cities

IoT has its major application in the smart home environments, where the enclosure of diverse gadgets allows the usual internal activities automation. Many applications of smart home environment suggested in the literature involved (wireless) sensors networks and carried out some smart metering proposals to contribute the identification of appliances, knowledge management of consumption of energy, lighting, heating and air conditioning. IoT can furnish a usual middleware for the future based smart city services retrieving data from various sensing infrastructure gaining all types of geo-location and IoT technologies. Various newly suggested solutions advice to utilize the Cloud architectures to provide the identification, connection, and combination of sensors and the actuators, so creating platforms are able to supply and support frequent connectivity and real-time applications for smart cities.

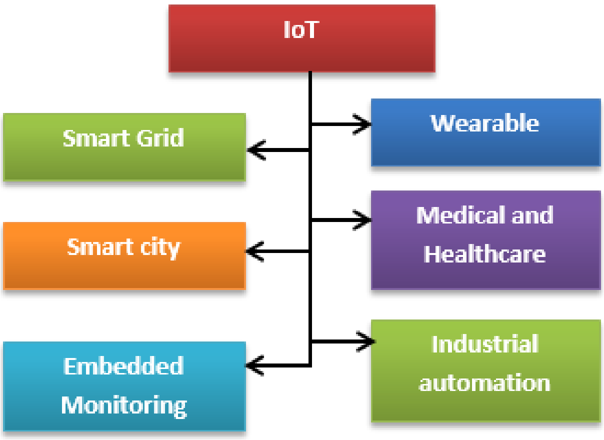


Fig.1: Applications of IoT

Healthcare

Smart devices, mobile internet and cloud services provide the continuity and organized invention of the healthcare and allow the cost effective, efficient, timely based and excellent quality of prevalent medical services. Those provided services involve management of chronic diseases, adult care and fitness events and so on.

Utilities

IoT application in the utilities domain includes actual time collection of used information, local balancing, forecasting demand and supply, generation of runtime tariff and so on; users connected to those smart networks was with the significant cost and resource savings.

Manufacturing

Remote monitoring and diagnostics, automation of production lines, handling the equipment and diagnostics via sensors placed on a production floor and so on are the few solutions recommended by IoT. The output ranges from optimized field support costs, reduces the breakdowns to increased operational efficiency.

Smart Mobility

As an increasing technology, the IoT is anticipated to give challenging solutions to modify transportation systems and also automobile services (like Intelligent Transportation Systems, ITS). A recent creation of IoT-related vehicular information Clouds can be evolved and provided to carry more business benefits, like improving road safety, minimizing road congestion, traffic management and suggesting car maintenance. Vehicles move with different speed frequencies results in intermittent interaction influencing the performance, reliability and also Quality of Service.

Challenges and Future of IoT

Technological improvements in IoT Meanwhile the achievable applications outlined above might be quite interesting, the demands administered the underlying technology may be considerable. Besides the prediction is that the technology is to be available with least costs, if many objects are actually to be equipped. We also faced many more other challenges scalability, Interoperability, Discovery, Security, Privacy, Fault tolerance, Power supply, Energy Efficient Sensing, Integration of data from multiple sources, Flexibility.

Future of Internet of Things (IoT)

Quality of Service: In Cloud computing, a QoS is another main research domain that requires high attention since the information and the tools are accessible on clouds. Dynamic scheduling and resource allocation paradigms based on the particle swam optimization are developed.

New Protocols: The protocol at the end of IoT performs a crucial role in total realization. They create a support for information tunnel between sensors and the external environment. An energy efficient MAC protocol and applicable routing protocol are important to a system for its efficiency working.

Virtualization: A contemporary visual technologies arise, creative visualization are enabled. The advancement from a CRT to a Plasma, LCD, and LED leads to highly efficient representation of data (using touch interface) with user and he is able to traverse the information better than before.

Cloud Computing: The integrated applications of IoT and the cloud computing allows the generation of the smart environments like smart cities is able to integrate services provided by the various stake holders and measure to support more users with good reliability and decentralized way.

III. INFORMATION ABSTRACTION

Under this section we discussed the terms of data abstraction on sensor information and its various ways of representation that involves multiple abstraction levels, its dissimilarities with other research domains and discussed motivation and the challenges in forming abstractions based on sensor data.

Abstraction

In the view of IoT the term abstraction has been coined in the context-aware computing domain, depicting the transformation of various levels of the context incorporation from sensing layer to perception layer [3]. That transformation process was defined by Chen and Kotz [4] as defining the top level context information from low level context (i.e. raw) sensor information through gathering, aggregating and inferring of raw information with extra knowledge by the environment with the motto of adjusting the behavior of sensor devices to recent context. The dual granularity abstraction levels with the objective of representing the knowledge with a user-centric focus: 1) lower level abstraction (or data abstraction) and 2) higher level abstraction (or semantic abstraction). The abstraction process as derived from the raw information to very valuable and understandable data. Lower level abstractions represent atomic and static data which is attained by collecting the data from individual local sensor data and by integrating that data with Meta data on local sensors like type, range, and capabilities. Mantyjarvi [5] explained this as a "smallest atomic quantity of context data with semantic meaning." Data abstraction can be attained via data processing approaches like pattern and event recognition that analyzes the raw sensor information of an individual node and notice to the user/network regarding the event happening. Higher level abstractions can be inferred by observing various sources of lower level abstractions to attain non-local image about happening activities and various events. Higher level abstractions can be attained by machine-learning approaches like classification and clustering of the lower level abstractions on time. Various approaches like logical inference by the help of the reasoning approaches and also rule-based systems are also utilized for such purpose. The representation form of abstraction may differ in several applications for sensor information.

Motivation for Information Abstraction

It has high demand for novel data processing approaches and the concepts to work with the risks in the problem of big data. We provide that data abstraction and that can be utilized to minimize information. Concentrating on abstracted data rather than the numerical data will bring two key advantages: 1) reduction of network traffic and 2) the improvement of comprehensiveness to the end-user. Rather transmitting the raw data to the user, abstracted data are less granular but concentrate on data, which might be useful to user. Data abstraction is used as a base for available approaches like outlier detection, activity recognition, and other emerging areas in the field of the sensor networks.

Limitations of IoT Devices

There are two major limitations on generic IoT Technologies. One is the battery capacity and the other is computing power.

Battery Life Extension

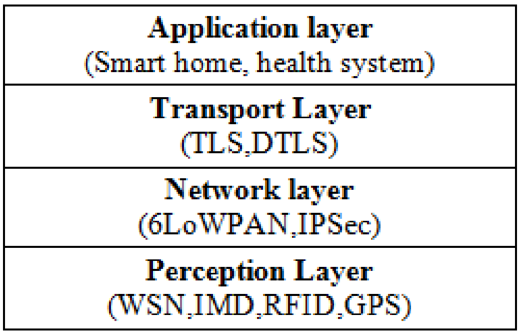
Some IoT devices are placed in locations where the charging is unavailable. Three approaches are possible in mitigating the issue of availability of charging. First thing is to utilize the fewer security requirements on a device that is not suggested particularly at the time of working with the sensible information. The second possible approach is to improve the capacity of battery. The third possible approach is saving energy from natural resources (ex: light, heat, vibration and wind).

Lightweight computation

The paper [9] stated that traditional cryptography will not work over the IoT systems, as the devices are having restricted memory space so that it is unable to manage the computing and storage essentials of advanced cryptography paradigms. In order to give support to security mechanisms of restricted devices, the researchers recommended that to reuse the available functions. For instance using the authentication of physical layer through the application of a signal processing at a receiver side is to verify whether the transmission is from the predicted transmitted in the desired location. On the other hand, particular analog transmitter features are effectively utilized for data encoding. The authors in [10] recommended an algorithm of encrypted query processing for IoT. This approach enables to store encrypted data of IoT very securely on cloud, and supports the efficient database query processing on encrypted information. In [11] authors introduced an approach to optimize latency for IoT when performing query processing on encrypted information by applying latency hiding technique, which consists of breaking down the query results of large size into small sized data sets. In [12] authors introduced a lightweight encryption scheme for smart homes based on stateful identity-based encryption (IBE), where the public keys are merely identity strings without the need for a digital certificate.

IV. SECURITY

Implementing the available standards of internet to the smart devices becomes easy to combine envisioned scenarios of IoT contexts. Moreover the security mechanisms in traditional Internet protocols are to be updated or extended in order to give support to the IoT applications. Under this section, we have discussed the problems in security and available answers in multiple layers in IoT systems (Figure 2).



Application layer
(Smart home, health system)

Transport Layer
(TLS,DTLS)

Network layer
(6LoWPAN,IPSec)

Perception Layer
(WSN,IMD,RFID,GPS)

Fig.2: Layers in IoT

IoT Perception Layer

An IoT system is developed to collect and exchange information in physical world. Therefore a perception layer has different kinds of gathering and handling the modules like temperature sensors, noise sensors, vibration sensors, pressure sensors and so on. This perception layer is further partitioned into two parts: a perception node (sensors or controllers, etc.), a perception network which communicates with the transportation network [7]. A perception node is utilized for the acquisition of data and its control, whereas perception network will send the gathered data to a gateway otherwise sends the control instruction to a controller. A Perception layer technology involves with WSNs, implantable medical devices (IMDs), radio-frequency identification, global positioning system, and so on. To attain the services quality, it is needed to find the incorrect nodes and corrective actions are taken to ignore next service degradation. Wang et al. [8] was derived the intrusion detection probability in the both homogeneous and heterogeneous WSN.

IoT Network Layer Security

For the devices of IoT in the context of WSN, it is required to prolong the IPv6 on powerless wireless PANs (6LoWPAN) to allow an IPSec interaction with the IPv6 nodes. This is an advantage since the prevailing end-points over the Internet are needed to be updated to interact securely with WSN, and the actual E2E security is implemented with no trustworthy gateway. Raza et al. [9] introduced an E2E secure communication between an IP enabled sensor networks and the conventional Internet and their extension to LoWPAN supports the both IPSec's authentication header and also Encapsulation Security Payload (ESP), so that the end points of communication authenticate, encrypt and check the integrity of text by using standardized and established IPv6 mechanisms.

IoT Transport Layer Security

Kothmayr et al. [11] proposed the first completely implemented a two-way authentication scheme to an IoT system, on the basis of available standards of internet, specifically a DTLS protocol. The presented security scheme is implemented at the time of completely authenticated DTLS handshake and depending on an exchanging of X.509 certificates having RSA keys. It will work on the standard communication stacks which provide an UDP/IPv6 networking for 6LoWPANs. Raza et al. [12] introduced 6LoWPAN header compression for DTLS. They linked with the compressed DTLS with the 6LoWPAN standard by using the standardized mechanisms. The proposed DTLS compression primarily minimizes some extra security bits. For instance, especially for a DTLS Record header which is included in each DTLS packet, some extra security bits will be ignored by 62%. In their further work [13], the integration of a DTLS and CoAP is introduced for an IoT and is named as Lithe. They also introduced a new DTLS header compression scheme for which the motto is to significantly minimize the consumption of energy by leveraging the 6LoWPAN standard.

IoT Application Layer Security

IoT has wide range of applications not only restricted to a smart home (e.g., learning thermostat, smart bulb) and it includes 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. Many recent devices of IoT are having configurable embedded systems. Whenever we connect them to internet they can infect by a computer virus as Trojan [14].

V. EARCHITECTURE & ELEMENTS

In the below sections we discuss the six major elements required to provide the functionality of an IoT as shown in Figure 3. In Table I we have shown the categorization of those elements and also examples of every category.

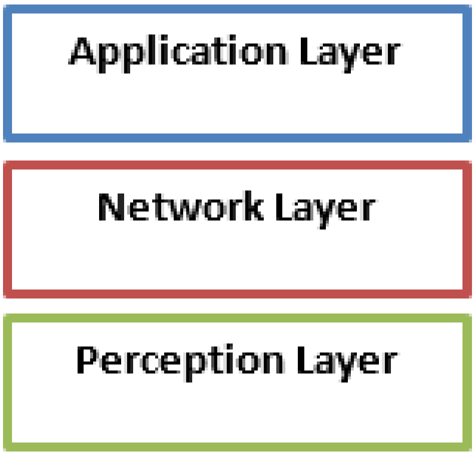


Fig.3: IoT Architecture

Identification

Identification is important to IoT to give identity and map the services depending on their demand. There exist different methods for IoT like Electronic Product Codes (EPC) and ubiquitous codes (uCode) [15]. Additionally it is difficult to address the IoT objects during differentiation between an object ID and the address of that object. An ID of the object denotes its name as "T1" for specific temperature sensor whereas the address of the object denotes it's self-address inside a communication network. Besides the IoT addressing methods involves IPv6 and IPv4.6LoWPAN [16] allows reduction mechanism on IPV6 headers which makes the IPV6 addressing as appropriate to powerless wireless networks.Identification methods are utilized to give a clear identity for every object inside a network. Additionally, whatever the objects those are inside the network may use public IPs instead private ones.

Sensing

The sensing in IoT refers to the collecting information from related objects of the internal network and sending it return to the data warehouse, database or cloud. We have to analyze the gathered information for taking particular actions on the basis of essential services. The IoT sensors might be sensors, actuators or wearable sensing devices. For example, some of the companies like Wemo, Revoly and Smart Things provide smart hubs and also mobile applications that allows people can monitor and manage more smart devices and the appliances which are in home by using their smartphones [17].

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, WiFi, WiFi 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

COMMUNICATION

In IoT the communication based technologies connect variety of objects together for delivering particular services. Usually, the nodes of IoT must be operated by using less power in presence of noisy and lost communication links. Some of the communication protocols used for IoT are WiFi, Bluetooth, IEEE 802.15.4, Z-wave and LTE-Advanced. Some particular communication technologies 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) [18].

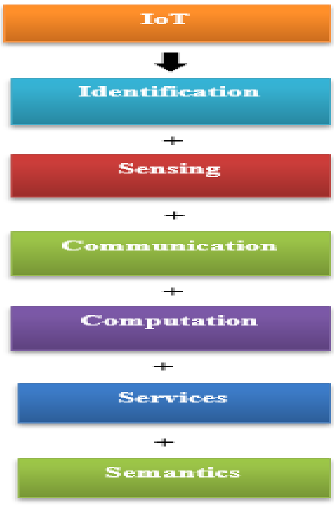


Fig.4: IoT Elements

Some Computation Processing units like microcontrollers, microprocessors, SOCs, FPGAs and the applications of software denotes the "brain" and IoTs computational ability. Many platforms in hardware are developed for running the applications of IoT like Arduino, UDOO, Friendly ARM, Intel Galileo, Raspberry PI, Gadgeteer, Beagle Bone, Cubieboard, Z1, Wi Sense, Mulle and T-MoteSky [19].

Semantics

In IoT semantic refers the ability to attain knowledge with ease through several machineries' to offer the essential services. Knowledge extraction involves finding and using the resources and data modeling. Besides it also includes finding and analyzing the data to take better decision for providing the actual service. Such requirement is supported by Semantic Web technologies like Resource Description Framework (RDF) and the Web Ontology Language (OWL). In 2011, the World Wide Web consortium (W3C) adopted the Efficient XML Interchange (EXI) format as a recommendation [20].

QoS

Comprehending the IoT vision is tough task since numerous challenges are to be mentioned. Few of the key challenges are availability, mobility scalability, security, trust, reliability, performance, interoperability, security and management. Mentioning those challenges allows the service providers and the application programmers to apply their services very efficiently.

Availability

The availability of IoT should be realized in both levels of hardware and software to offer services anywhere and anytime for customers. The software availability mentions the capability of IoT applications for providing the services to everyone at various locations concurrently. The hardware availability mentions the availability of gadgets every time which are compatible with IoT functionalities and its protocols like IPv6, 6LoWPAN, RPL, CoAP and so on. These protocols must be sink to the devices restricted with a single board resource internally that deliver the functionality of IoTs.

Reliability

It refers to the systematic processing of a system on the basis of its specification [21]. It aims at improving the rate of success in delivery of IoT services. It is very close with availability and reliability, we guarantee's the data availability and the services on time. Here the hardest part is that a communication network that must be flexible with the failures so that to realize the distribution of reliable data.

Mobility

Mobility is another challenge of IoT applications since many services need to be delivered to mobile users. The interruption during services to mobile devices occurs when such devices shifts from one gateway to the. [22] Presents a resource mobility scheme that allows two modes: namely caching and tunneling for supporting services continuity. These modes enable the applications to access the IoT information over temporary unavailability of resources. Several smart devices of IoT systems also need some efficient techniques for the mobility management.

Performance

Assessing the performance of IoT services is a great challenge since it relies on many components performance. Similar to other systems, the IoT requires developing and increasing its services to accomplish the customer's requirements. The devices of IoT must be monitored and also be evaluated to give excellent performance for reasonable costs for consumers. Several metrics are used to evaluate the IoT performance that includes speed, form factor of that device and cost.

Scalability

The IoT scalability refers as the ability to include new gadgets, services and functions for users without having negative impact on the quality of available services. Appending new functions and assisting new gadgets is not that much easy thing particularly when there are different platforms and communication protocols. The applications of IoT should be modeled from base to allow additional services and functions.

Interoperability

End-to-end interoperability is one more challenge of IoT for handling more varieties of objects belonging to multiple platforms. Interoperability must be compared by both the application developers and manufactures of IoT devices to attain the conveyance of services to all users nonetheless of their using hardware platform requirements. For instance, many smartphones in todays' support basic communication technologies like Wi-Fi, NFC, and GSM to assure interoperability in various scenarios.

Security and Privacy

Security gives a key challenge for implementing IoT because of deficit of general standard and the architecture of IoT security. In diverse networks of IoT is not much easier to guarantee the user's security and also their privacy. The basis functionality of an IoT is data exchanging between billions of connected objects through internet.

VI. CONCLUSION

IoT as the name says is a wireless network consist of huge number of interconnected things which communicates each other without human involvement i.e. using sensors. Smart Home, Healthcare, Utilities, Manufacturing, Smart cities and automation and smart mobility are the few applications and classified on the type of network availability, scale. The technologies such as RFID, WSN are used to meet such kind of challenges. This paper is mainly concentrated on the key aspects such as issues, applications, literatures gaps and challenges faced in IoT. We discussed information abstraction at different levels from the raw data collected from the sensors. The security at different layers in the architecture of IoT such as in application, transport, network, perception layer along with the basic IoT elements. The limitations of the computing devices such as battery power and computing capacity are discussed and yet to be a good scope in search. The challenging aspects in the view of Quality of service such as availability, reliability, mobility, scalability are also addressed.

VII. 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]. 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

[5]. J. Mantyjarvi, Sensor-Based Context Recognition for Mobile Applications. Espoo, Finland: VTT, 2003.

[6]. M. Compton et al., "The SSN ontology of the W3C semantic sensor network incubator group," Web Semant. Sci. Serv. Agents World Wide Web, vol. 17, pp. 25–32, 2012.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," IEEE Sensors J., vol. 13, no. 10, pp. 3711–3720, Oct. 2013.

[14]. 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.

[15]. 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.

[16]. 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.

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

[18]. 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.

[19]. 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.

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

[21]. D. Macedo, L. A. Guedes, and I. Silva, "A dependability evaluation for Internet of Things incorporating redundancy aspects," in Proc. IEEE 11th ICNSC, 2014, pp. 417–422

[22]. 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.

Authors Profile:

Ms. B. Mounika, currently working as Assistant Professor at AITS, Rajampeta. She received her master's degree in Computer Science and Engineering from SVIST College of Engineering, Kadapa in the year 2015. She received her Bachelor's degree in computer science and engineering from Vaagdevi Institute of Technology and Science, Proddatur affiliated to JNTUA University in 2012. Her areas of interest include Internet of Things and Big Data.

Ms. B. Mamatha, currently working as Assistant Professor at KLM College of Engineering for Women, Kadapa. She received her master's degree in Computer Science and Engineering from KSRM, Kadapa in the year 2015. She received her Bachelor's degree in Computer Science and Engineering from KSRM, Kadapa affiliated to S.V University in 2009. Her areas of interest include Internet of Things and wireless networks, Network Security and Cryptography.