International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 5, Issue 3 (September '2019)

INTERNET OF THINGS: VISION, TECHNOLOGIES AND CAPABILITIES FOR EFFECTIVE LEARNING AND RESEARCH WITH SECURITY ISSUES

Gulshan Kumar,
Assistant Professor in Computer Department,
Swami Premanand Mahavidyalaya (SPN College),
Mukerian, Punjab, India.

Abstract: The internet of things (IoT), also called internet of all, is a new paradigm that combines several technologies such as computers, the internet, sensors network, radio frequency identification (RFID), communication technology and embedded systems to form a system that links the real worlds with digital worlds. IoT represents a system which consists things in the real world, and sensors attached to or combined to these things, connected to the Internet via wired and wireless network structure. The IoT sensors can use various types of connections such as RFID, Wi-Fi, Bluetooth, and ZigBee, in addition to allowing wide area connectivity using many technologies such as GSM, GPRS, 3G, and LTE. By the technology of the IoT, the world will becomes smart in every aspects, since the IoT will provides a means of smart cities, smart healthcare, smart homes and building, in addition to many important applications such as smart energy, grid, transportation, waste management and monitoring . In this paper we review a concept of many IoT applications and future possibilities for new related technologies in addition to the challenges that facing the implementation of the IoT.

Keywords: Internet of Things, ARPANET, ICANN, Radio Frequency Identification, WSN, Cloud Computing, Embedded Systems, Smart Object.

I. INTRODUCTION

The Internet of Things (IoT) sometimes referred to as the Internet of Objects, will change everything including ourselves. The Internet has an impact on education, communication, business, science, government, and humanity [1]. Clearly, the Internet is one of the most important and powerful creations in all of human history and now with the concept of the internet of things, internet becomes more favorable to have a smart life in every aspect[2].

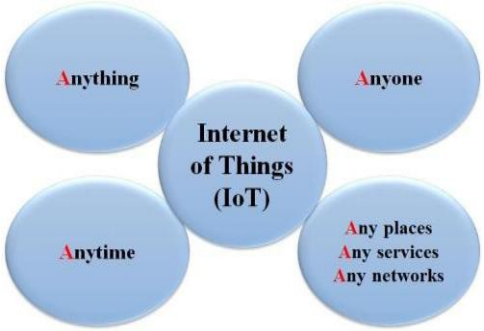

Figure 1. Internet of things Concept

Internet of Things is a new technology of the Internet accessing. By the Internet of Things, objects recognize themselves and obtain intelligence behavior by making or enabling related decisions thinks to the fact that they can communicate information about themselves [3]. These objects can access information that has been aggregated by other things, or they can add to other services [3]. Figure 1 reviews that with the internet of things, anything's will able to communicate to the internet at any time from any place to provide any services by any network to anyone. this concept will create a new types of applications can involve such as smart vehicle and the smart home, to provide many services such as notifications, security, energy saving, automation, communication, computers and entertainment [4].

By developing the IoT technology, testing and deploying products it will be much close to implementing smart environments by 2020 [6]. In the near future, storage and communication services will be highly pervasive and distributed: people, machines, smart objects, surrounding space and platforms connected with wireless/wired sensors, M2M devices, RFID tags will create a highly decentralized resources interconnected by a dynamic network of networks[7].

In the IoT, the communication language will be based on interoperable protocols, operating in heterogeneous environments and platforms [8]. IoT in this context is a generic term and all objects can play an active role to their connection to the Internet by creating smart environments, where the role of the Internet has changed[9]. Section I contains the introduction of IoT. Section II discuss about the Architecture of IoT. Section III contains Internet of Things (IoT) Technologies. Section IV in this Section discuss about the various Standard and protocols. In the Section V describes The Internet as a Research Tool. Section VII contains the security issues of IoT.

II. IoT ARCHITECTURE

The IoT can be capable of interconnecting various heterogeneous objects through the Internet, so there is a need for a flexible layered architecture. The figure (2) illustrates the 3-layer architecture of IoT.

IJCRCST © 2019 | All Rights Reserved

The basic model is a 3-layer architecture consisting of the Application, Network, and Perception Layers. In the recent literature abstraction is added to the IoT architecture [3].

Objects Layer: The first layer is objects or perception layer, it represents the sensors used in IoT that collect and process information. The perception layer includes sensors and actuators. The sensors and actuators perform different functionalities such as identifying temperature, motion, location, weight, humidity, vibration, acceleration etc. This layer digitizes and transfers data to the Object Abstraction layer. The perception layer transfers data through secure channels. The perception layer initiates the big data created by IoT. [3] This layer gives a physical meaning to each object. Object layer consists of data sensors in the form of RFID tags, IR sensors or other sensor networks which can be able to sense the temperature, speed, humidity, location and so on. Object layer gathers the useful information of objects from the sensor devices which is connected to those objects and converts the information into digital signals. Then the digital signal is passed to network layer [4]. The Perception layer is nothing but collection of sensor, actuators which forms WSN [6].

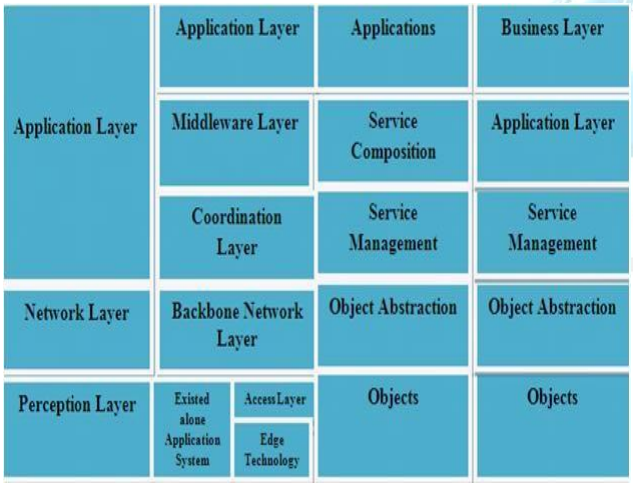

Figure 2: The IoT Architecture (a) Three Layer (b) Middle-ware based Layer (c) SOA based Layer (d) Five-layer

Object Abstraction Layer: The Object Abstraction layer transfers data to the Service Management layer produced by perception layer through secure channels. Data can be transferred through RFID, 3G, Wi-Fi, GSM, ZigBee, Bluetooth etc. Cloud computing and data management processes are done by Object Abstraction Layer [3].

Service Management Layer: The next layer is Service Management or Middleware layer. This layer pairs a service with its requester based on addresses and names. Service Management layer processes the data received, makes decisions and delivers the services required. The Service Management layer also allows the IoT application programmers to work with heterogeneous objects without any consideration to a specific hardware platform [3]. Information received from the sensor devices is processed by Service Management Layer. The information is processed using some Intelligent Processing Equipment. Based on the processed results of the information fully automated action is taken [4].

Application Layer: This layer provides the services requested by customers. For example, it provides the temperature and air humidity measurements to customer. Application provides high quality smart services to meet customer needs [3]. Application layer is very helpful in the large scale development of IoT network. Application related to IoT could be smart homes, smart transportation, smart planet and son on [4]. It is a top most layer which consists of business logic, formulas and UI to user end [6].

Business Layer : This layer manages the overall IoT system services and activities. Business Layer builds a business model, graphs, flowcharts etc based on data received by Application Layer. The Business Layer also implements, design, monitor, analyze and develop the elements related to IoT. This layer supports decision making processes based on Big Data analysis. Business Layer also monitors and manages the underlying four layers. It also compares the output of each layer with expected output to enhance services [3]. For effective business strategies it generates different business models [4].

III. INTERNET OF THINGS TECHNOLOGIES

A novel paradigm called Internet of Things (IoT) has rapidly gained ground in recent years. IoT refers to "a global network of interconnected objects that are uniquely addressable based on standard communication protocols", the point of convergence of which is the Internet. IoT is powered by the latest advances in a variety of communication devices and technologies, but the things included in IoT are not just complex devices such as mobile phones, but they also include everyday objects such as food, clothing, furniture, paper, landmarks, monuments, works of art, etc.. These objects, acting as sensors or actuators, are capable of interacting with each other to achieve a common goal. In the following, we describe some very important technological aspects related to the IoT.

RFID Technology (Radio Frequency Identification): RFID is an automatic and contactless technology, providing a communication interface with the tagged objects through wireless data transmission to retrieve relevant information [20]. Radio frequency identification (RFID) allows automatic identification and data capture using radio waves, a tag, and a reader. The tag cab store more data than traditional barcodes. Three types of tags are used.

Passive RFID tags rely on radio frequency energy transferred from the reader to the tag to power the tag; they are not battery-powered. Passive RFID technologies present many advantages. Indeed, RFID can be seen as "electronic bar codes" which do not need objects to be handled one by one. In addition, no direct sight is necessary. More and more information can be stored in tags. Tag reading is quick (a reader can read up to 200 tags per second) [20]. Applications of these can be found in supply chains, passports, and electronic tolls.

Active RFID tags can contain external sensors to monitor temperature, pressure, chemicals, and other conditions.

Active RFID tags are used in manufacturing, hospital laboratories, and remote-sensing IT asset management. Semi-passive RFID tags use batteries to power the microchip while communicating by drawing power from the reader. Active and semi-passive RFID tags cost more than passive tags.

In IoT scenario, a key role is played by RFID systems, composed of one or more readers and several tags. These technologies help in automatic identification of anything they are attached to, and allow objects to be assigned unique digital identities, to be integrated into a network, and to be associated with digital information and services.

Wireless Sensor Networks (WSN): A Wireless Sensor Network (WSN) can be defined as a network of small embedded devices, called sensors, which communicate wirelessly following an ad hoc configuration [20]. Wireless sensor networks (WSN) consist of spatially distributed autonomous sensor- equipped devices to monitor physical or environmental conditions and can cooperate with RFID systems to better track the status of things such as movements, pressure, temperature, and location. Wireless sensor networks (WSN) my provide various useful data and are being utilized in several areas like healthcare, government and environmental services (natural disaster relief), defense (military target tracking and surveillance), hazardous environment exploration, seismic sensing. (WSN) are used for maintenance and tracking systems. For example, General Electric deployed sensors in its jet engines, turbines, and wind farms. By analyzing data in real time, General Electric saves time and money associated with preventive maintenance. Likewise, American Airlines uses sensors capable of capturing 19 terabytes of data per flight for services such as preventive maintenance.

Middleware: Middleware is a software layer interposed between software applications to make it easier for software developers to perform communication and input/ output. Middleware gained popularity in the 1980 due to its major role in simplifying the integration of legacy technologies into new ones. It also facilitated the development of new services in the distributed computing environment. A complex distributed infrastructure of the IoT with numerous heterogeneous devices requires simplifying the development of new applications and services, so the use of middleware is an ideal fit with IoT application development. For example, Global Sensor Network (GSN) is an open source sensor middleware platform enabling the development and deployment of sensor services with almost zero programming effort. Due to the heterogeneity of the participating objects, to their limited storage and processing capabilities and the huge variety of applications involved, a key role is played by the middleware between the things and the application layer, whose main goal is the abstraction of the functionalities and communication capabilities of the devices. The middleware can be divided in a set of layers: Object Abstraction, Service Management, Service Composition, and Application [20].

Cloud Computing: The essential aspects of cloud computing have been reported in the definition provided by the National Institute of Standard and Technologies (NIST): "Cloud computing is a model for on demand access to a shared pool of configurable resources (e.g., computers, networks, servers, storage, applications, services, software)" that can be provisioned as infrastructure as a service or software of the IoT is an enormous amount of data generated from devices connected to the internet.

IV. INTERNET OF THINGS STANDARDIZATIONS AND PROTOCOLS

By the 2020 around 50 to 100 billion things will be connected electronically by internet [10]. Figure (3) shows the growth of the things connected to the internet from 1988 to forecast 2020. The Internet of Things (IoT) will provide a technology to creating the means of smart action for machines to communicate with one another and with many different types of information [11]. The success of IoT depends on standardization, which provides interoperability, compatibility, reliability, and effective operations on a global scale [12]. Today more than 60 companies for leading technology, in communications and energy, working with standards, such as IETF, IEEE and ITU to specify new IP based technologies for the Internet of Things [13].

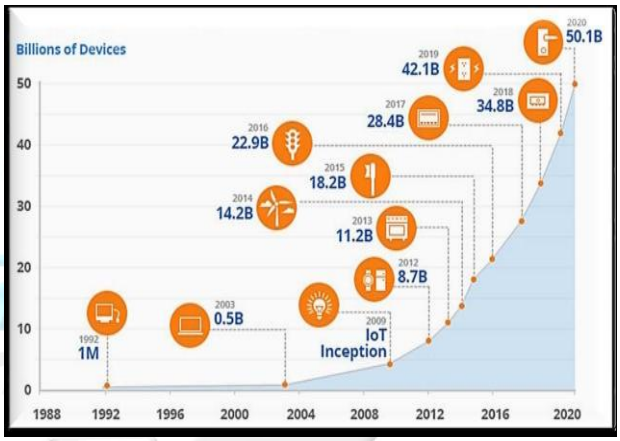

Figure 3 : Internet of Things Growth

The design of the IoT standards is required to consider the efficient use of energy and network capacity, as well as respecting other constraints such as frequency bands and power levels for radio frequency communications [14]. As IoT evolves, it may be necessary to review such constraints and investigate ways to ensure sufficient capacity for expansion, for example in case of additional radio spectrum allocation as it becomes available [16]. IEEE Standards Association (IEEE-SA) develops a number of standards that are related to environment need for an IoT. The main focus of the IEEE standardization activities are on the Physical and MAC layers [17]. The IEEE provides an early foundation for the IoT with the IEEE802.15.4 standard for short range low power radios, typically operating in the industrial, scientific and medical band in addition to use ZigBee technology [18]. The IEEE-SA has an over 900 active standards and more than 500 standards under development. In its research into IoT, it has identified over 140 existing standards and projects that are relevant to the IoT. The base project related to IoT is IEEE P2013 which it is currently considering the architecture of IoT [19].

V. THE INTERNET AS A RESEARCH TOOL

The internet indeed possesses great power. The invention amasses great features and opportunities that cannot be

ignored or snubbed. Other spheres of human endeavors have not snubbed it, and the sciences would not either. In this Information Technology age, conscious of the invaluable roles and contributions of the internet to global development, we argue that scientific research can only get better if like others, it pitches it tent with technology, specifically Internet Technology, leveraging the powerful features and openings the internet promises and unveils.

INFORMATION AGGREGATION: The internet domain offers easy access to nearly limitless information. With the global connectivity of millions of servers harboring data and information, access to the internet implies access to these servers for resources required to meet scientific research ends. And, obviously, information gathering is sustained mostly by search engines (Google, yahoo, msn, Ask etc), specialist websites, and aggregation engines (e.g., folk simonies like Flicker, or YouTube), and specifically by scientific data-mining services (e.g., Google Scholar and Web of Science in biblio-metrics) [20]. Unlike in the past, Information currently available on the internet take different forms ranging from text-only data, audio and video formats etc. these could be acquired depending on user needs, skills and search proficiency. The concept of optimized search otherwise referred to as 'search engine optimization, SEO' has helped simplify further the ease at which specified information can be derived from the internet. SEO phenomenon projects an art as well as a science of helping or aiding easy and speedy location of information on major searches.

COMMUNICATION AND COLLABORATION: Communication is typically the act of sending messages; which again an important activity is in scientific research. Conventionally, this is achieved via manual/paper, hard-copy mails (post office letters, memo etc) to research associates to communicate and (or) exchange research findings or requests, which traditionally takes a sluggish turn, slowing the general research process. However, with the internet, communication with colleagues around the world has increased in speed and quality.

Since the launch of electronic-mail (e-mail), and given the small bandwidth requirement for emails and its mostly text only nature, e-mails are about the most widely used internet service; allowing for easy and cost effective access by many research centers and educational institutions. E-mailing is noted to be considerably the most common internet activity, with about 90% of all internet user claiming to be active e-mailers in [20]. Interestingly, newer technological developments in the forms of social networking, and the recurrent improvements in connection speed and bandwidth usage for, paving way for the emergence and adoption VoIP systems (Skype, Tango, etc) that allow for hosting virtual meetings and research collaborations without much technical difficulties.

DATA SELECTION AND ANALYSIS: The art of collecting data or sample data selection is an indispensable part of scientific research process. And of course, this is submitting to unparalleled historical transformation in scale and number of opportunities in the sciences [19]. Just like the traditional methods of data collection and (or) selection (surveys, interviews, questionnaires, etc), the internet provides for the extension of such processes into the digital space. Today, with the use of various web application technologies like HTML, XML, PHP, ASP, etc, and 'killer applications' and VoIP schemes, researchers can convenient reach out and in fact harness desired research data from varying respondents with predefined analytical structures that enables the ease of making inferences without much difficulty.

PUBLISHING: Publishing is another facet of research that has witnessed tremendous change with internet influence. Computerization and (or) digitization has affected automation, workflow and publishing process integration readily expressed in forms of blogging and social / cross media. The most alluring advantage of this developmental phenomenon is the potential riddance of the formerly difficult requirements (elongated publications processing including payment modes) that often delayed or even repressed the unrestricted flow of research submissions and communications Even more interesting, is the fact that scientific researchers and their institutions are fast tending towards embracing online and (or) open access publishing and institutional or individual self-archiving. In physics as an instance, the process was initiated quite early and is near completion, credits to formidable, strong- willed efforts of enterprising individuals in [18].

RESEARCH AND GRANTS ACQUISITIONS: Grant Acquisition is yet another aspect of academic research that has leveraged on the strengths of the internet. Usually, grants follow laid down processes that have enjoyed simplification with the emergence and use of the internet. Online learning concept is diffusing; and this is eagerly being incorporated into research activities. Today, Funding and (or) research donor agencies convey research interests and guidelines through their websites, funding applications, proposals, and other research requisitions can be submitted via online mediums (online forms and emails), grants and research sponsorship procedures can also be accessed online thanks to the online capabilities of e-banking. Given that research evolves and it processes are continuous, we suggest this model should assume a recurrent nature, as might be considered necessary to ensure invaluable output. Hence, the arrow signifies potential transitions from one stage to the order, which could be repeated as many times as possible following the goals of result improvement or upgrade.

VI. SECURITY ISSUES IN IOT

Internet is key infrastructure of IoT hence there is a possibility for some prominent security issues [5]. IoT is a collection of physical objects connected to internet; hence many security issues may occur. Some of the security issues are:

Security issues in perception layer: It is a lowest level of IoT construction. Perception layer is the source of access to information throughout the IoT. The security issues in Perception layer include physical security of sensing devices and security of information collection. IoT cannot provide a security protection system and it is vulnerable to the attack

due to diversity, energy limited, simple and weak protective capability of sensing node which affects the security of WSN, RFID and M2M terminal. The RFID includes security problems such as information leakage, replay attacks, information tracking, tampering, cloning attacks and man-in-the- middle attacks. The security problems faced in perception layer includes capture gateway node, physical capture, unfair attacks, congestion attack, DoS attacks, node replication attack and forward attack [8].

Security issues in the wireless sensor networks (WSNs): WSN is a network of nodes that sense and control the environment. It also enables the interaction between persons or computers and the surrounding environment. WSN includes sensor nodes, actuator nodes and so on. WSN is a collection node hence there is a possibility of security issues. The operations performed in a wireless sensor network can be categorized under three categories [5]:

i. Attacks on secrecy and authentication
ii. Silent attacks on service integrity
iii. Attacks on network availability

Security issues in RFID technology:
In IoT, RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement. The RFID tags are vulnerable to various attacks from outside due to the incorrect security status of the RFID technology [5]. The four most common types of attacks and security issues of RFID tags are as follows:

i. Unauthorized tag disabling: In this DoS attacks the RFID tags will become incapable temporarily or permanently. Such attacks make RFID tag available to malfunction and misbehave under the scan of a tag reader. These attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

ii. Unauthorized tag cloning: Capturing the identification information through the manipulation of the tags by dishonest readers falls under this category. Once the identification information of a tag is compromised, replication of the tag is made possible which can be used to bypass fake security measures as well as introducing new vulnerabilities using RFID tags automatic verification steps [5].

iii. Unauthorized tag tracking: The dishonest readers can trace the tag, which results in giving the sensitive information, for example person's address. Thus from the viewpoint of customer, buying a product which is having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and in fact endangers their privacy.

iv. Replay attacks: In Replay attacks the attacker uses a tag's response to a dishonest reader's challenge to impersonate the tag. In these attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag.

Security issues in physical layer:
The physical layer performs different functionalities such as selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, transmission and reception of data [6]. This layer is attacked mainly through

i. Jamming: This DoS attack occupies the communication channel between the nodes and prevents them from communicating with each other. It exploits the transmission of radio signal to interfere with radio frequencies that used by sensor network. It can be performed either continuously or in an isolated way [7]. In both the cases network will suffer from damage.

ii. Node tampering: Extracting sensitive information is known as node tampering.

Security issues in network layer:
Internet of things faces some risk in the network like illegal access, confidentiality, data eavesdropping, integrity, DoS attacks, destruction, virus attack, man-in-the-middle attack and so on. IoT sensing a large number of devices hence a variety of formats of the data collected, and the data information has a massive, multi-source and heterogeneous characteristics. It will also causes network security issues like data transfer needs of large number of nodes leading to network congestion, resulting in DoS attacks [8]. The function of the network layer is routing [5]. The DoS attacks taking place in the network layer:

i. Hello flood attack: Hello flood attack causes high traffic in channels by congesting the channel with a high number of useless messages unusually. Here a single malicious node sends a useless message then that message is replayed by the attacker to create a high traffic.

ii. Homing: In this attack, a search is made in the traffic for cluster heads and key managers which having the capability to shut down the entire network.

iii. Selective forwarding: In this, a compromised node sends few selective nodes instead of all the nodes. The selection of the nodes is based on the requirement of the attacker to achieve his malicious objective and thus such node does not forward packets of data.

iv. Sybil: In this attack, the attacker replicates a single node and then presents it with multiple identities to the other nodes.

v. Wormhole: Wormhole attack causes relocation of bits of data from its original position. The relocation of data packet is carried out while passing bits of data over a link of low latency.

vi. Acknowledgement flooding: When routing algorithms are used then the acknowledgements are required at times in sensor networks. In Acknowledgements flooding attack, a malicious node spoofs the acknowledgements providing false information to the destined neighboring nodes.

Security issues in application layer:
Application of IoT is the result of closely integration between communication technology, computer technology and industry professional which can be able to find applications

in many aspects. The security issues in application layer include eavesdropping and tampering [8]. This layer carries out the responsibility of traffic management. It also provides software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries [5]. A path-based DoS attack is initiated in application layer by stimulating the sensor nodes to create a huge traffic in the route towards the base station.

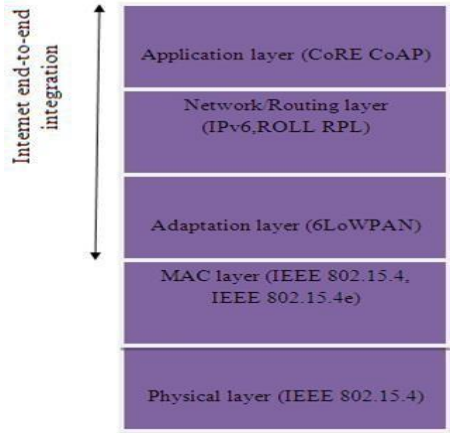

Figure 4: Communication protocols in the IoT

The figure (4) illustrates the communication protocols in the IoT. The protocols that support internet communication with sensing devices in IoT [9].

SECURITY REQUIREMENTS: Security in IoT is a need of the time. Security must provide integrity, confidentiality, non-repudiation and authentication of the information flows. Security of IoT communications can be addressed in the context of the communication protocol, or on the other end by external mechanisms. Other security requirements should be considered for the IoT and in particular regarding communications with sensing devices. Some mechanisms are also required to implement protection against threats to the normal functioning of IoT communication protocols. For example, fragmentation attacks at the 6LoWPAN adaptation layer. Some other relevant security requirements are anonymity, privacy, trust and liability which will be fundamental for the social acceptance of most of the future IoT applications employing Internet integrated sensing devices.

VII. CONCLUSIONS

Internet of things is a new technology which provides many applications to connect the things to things and human to things through the internet. Each object in the world can be identified, connected to each other through internet taking decisions independently. All networks and technologies of communication are used in building the concept of the internet of things such technologies are mobile computing, RFID, wireless sensors networks, and embedded systems, in addition to many algorithms and methodologies to get management processes, storing data, and security issues. IoT requires standardized approach for architectures, identification schemes, protocols and frequencies will happen parallels, each one targeted for a particular and specific use. by the internet of things many smart applications becomes real in our life , which enable us to reach and contact with every things in addition to facilities many important aspects for human life such as smart healthcare, smart homes, smart energy , smart cities and smart environments.IoT with particular focus on what is being actually done in addition to the challenges that facing the implementation the internet of things concept, and the other future technologies make the concept of IoT feasible.

VIII.REFERENCES

[1]. M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (Iot): A Scalable Approach to Connecting Everything. *The International Journal of Engineering and Science* 4(1) (2015) 09-12.
[2]. http://www.meraevents.com/event/iot-workshop
[3]. http://www.nxp.com/assets/documents/data/en/white-papers/INTOTHNGSWP.pdf
[4]. Saranya C. M., Nitha K. P., Analysis of Security methods in Internet of Things. *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume 3, Issue 4; April 2015.
[5]. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, 2013 Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 1645-1660.
[6]. Daoliang Li, Yingyi Chen, Oct. 2010, Computer and Computing Technologies in Agriculture. Springer, 20-19.
[7]. L. Atzori, A. lera, G. Morabito, The Internet of Things: Survey. Computer networks, 1987–1905.
[8]. Internet of Things, 2014 http://postscapes.com/internet-of-things-history.
[9]. Huansheng Ning, Hong Liu, 2012 Cyber-Physical-Social Based Security Architecture for Future Internet of Things, Advances in Internet of Things, 1-7.
[10]. R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference On, 2012, pp. 207- 190.
[11]. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Comput. Syst., vol. 19, pp. 1645-1660, 2013.
[12]. P. Lopez, D. Fernandez, A. J. Jara and A. F. Skarmeta, "Survey of internet of things technologies for clinical environments," in Advanced Information Networking and Applications Workshops (WAINA), 2013 19th International Conference On, 2013, pp. 1199-1194.
[13]. D. Yang, F. Liu and Y. Liang, "A survey of the internet of things," in Proceedings of the 1st International Conference onE-Business Intelligence (ICEBI2010), 2010, pp. 198-196.
[14]. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton and T. Razafindralambo, "A survey on facilities for experimental internet of things research," Communications Magazine, IEEE, vol. 49, pp. 58-67, 2011.
[15]. Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," Wireless Communications, IEEE, vol. 20, pp. 91-98, 2013.

[16]. Y. Huang, Z. Yang, S. Xiong "Design and Implementation of A Bicycle Parking System Based on Internet-of-things" National Conference on Information Technology and Computer Science (2012). Pp: 593 – 596.
[17]. Bielsa (2012, Feb.10) Smart Water project in Valencia to monitor Water Cycle Management [Online]
[18]. Available: http://www.libelium.com/smart_water_cycle_monitoring_sens or_network/
[19]. Q. Wei, S. Zhu, C. Du, "Study on key technologies of Interne of Things perceiving mine," Procedia Engineering, vol.19, pp.2019-2019, 2011.
[20]. B. Karakostas, "A DNS architecture for the Internet of Things: a case study in transport logistics," Procedia Computer Science, vol.19, pp.594-601, 2013.
[21]. Y. Zhang, B. Chen, and X. Lu, "Intelligent monitoring system on refrigerator trucks based on the Internet of Things," Wireless Communications and Applications, vol.72, pp.201- 206, 2012.

Authors Profile

Mr. Gulshan Kumar completed Bachelor of Computer Applications from Panjab University Chandigarh, in year 2012 and Master of Computer Applications from Panjab University in year 2015. He is currently working as Assistant Professor in Department of Computer Applications at Swami Premanand Mahavidayalaya (S.P.N. College) Mukerian under the affilattion of Panjab University Chandigarh since 2016. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, IoT and Blockchain Technology. He has more than three years of teaching experience.