A Literature Survey on IoT Security Challenges

Shubhalika Dihulia
M. Tech Student
Department- C.S.E
All Saints college of Technology,
Bhopal, India

Tanveer Farooqui
Assistant Professor
Department- C.S.E
All Saints college of Technology,
Bhopal, India

ABSTRACT
This survey paper discuss the security challenges in IoT network. IoT is hot research topic in between researchers. In the era of digital media IoT play an important role of information servers and data warehouses. IoT network are used in different cities of smart city network. That's why the security of the IoT network is also a big task. There are many loop holes available in IoT based security network. In this survey paper discuss the security aspects in the IoT networks. Also discuss the different researches previous work and previous work in IoT security. This survey analyzes existing protocols and mechanisms to secure communications in the IoT, as well as open research issues. We analyze how existing approaches ensure fundamental security requirements and protect communications on the IoT, together with the open challenges and strategies for future research work in the area. This is, as far as our knowledge goes, the first survey with such goals.

Keywords
End-to-end security, IEEE 802.15.4, Internet of things, RPL, Security, MAC layer, IP V6 and V4

1. INTRODUCTION
The deepest technologies are those that are disappearing and are being woven into the fabric of everyday life until they are not distinguished from it" was Mark Weiser's central statement in his seminal paper in Scientific American 1991. There is a radical change in the daily life of man as well as in working conditions in organizations after the arrival of IT and ITeS technologies. This becomes a well-known concept in many horizontal and vertical markets, including the everyday life of a common man in society, as it has several applications. The development of Internet of Things [IoT] has been driven mainly by the needs of large enterprises that benefit greatly from the foresight and predictability offered by the ability to track all objects through the product chains in which they are integrated [1]. The ability to code and track objects has enabled organizations to become more efficient, accelerate processes, reduce errors, prevent theft and integrate complex and flexible organizational systems via IoT [2]. IoT is a technological revolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important areas, from wireless sensors to nanotechnologies. They will tag each object to identify, automate, monitor and control.

2. INTERNET OF THINGS (IOT)
Internet of Things is a new paradigm shift in the IT arena. The term "Internet of Things", which is also known as IoT, is invented from the two words, that is, the first word is "Internet" and the second word "Things". The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP / IP) to serve thousands of users worldwide. It is a network of networks composed of millions of private, public, academic, commercial and government networks, with global reach, linked by a wide range of electronic, wireless and optical network technologies. Today, more than 100 countries are linked to the exchange of data, news and opinions via the Internet. According to global Internet statistics, as of December 31, 2011, there were about 2,267,233,742 Internet users worldwide (data accessed dated 06/06/2013: from Universal Resource Location http: //www.webopedia COM / TERM / I / Internet.html). This means that 32.7% of the world's total population uses the Internet. Even the Internet is going into space thanks to Cisco's Internet Routing in Space (IRIS) program in the next four years (accessed on 10/05/2012:

(http://www.cisco.com/web/strategy/government/ In order to arrive at things that can be an object or a person who can be distinguished by the real world, everyday objects include not only the electronic devices that we encounter and use everyday and technologically advanced products Such as equipment and gadgets, but "things" that we do not normally do as electronic, such as food, clothing and furniture, materials, parts and equipment, goods and specialized items, Monuments, works of art and all the diversity of commerce, culture and sophistication. [4] This means that things can be both living beings such as the person, the cow v Water, dogs, pigeons, rabbits etc., plants-mango, jasmine, banyan, etc., and non-living things like chair, refrigerator, light tube, curtain, plate, etc. Ances or apparatus of the industry. So, at this stage, things are real objects in this physical or material world. The best definition for the Internet of things would be: "An open and comprehensive network of intelligent objects that have the ability to organize, share information, data and resources, respond and act in situations and Changes in the environment.

3. IoT TECHNOLOGIES
3.1 Internet of Things (IoT): A vision, architectural elements, and future directions
In 2013, Jayavardhana et al "Internet of Things (IoT): A vision, architectural elements, and future directions". The ubiquitous detection activated by wireless network technologies (WSN) covers many areas of modern life. This makes it possible to measure, infer and understand environmental indicators, delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communication actuation network creates Internet of Things (IoT), where sensors and actuators blend perfectly with the environment around us and information is shared across platforms to develop A common operational image (COP). Thanks to the recent adaptation of a variety of enabling wireless technologies such as RFID tags and integrated sensors and actuator nodes, IoT has emerged from its infancy and is the next breakthrough technology in transforming the Internet into A fully integrated Future

Internet. As authors move from www (static web pages) to web2 (social networking) to web3 (ubiquitous computer web), the need for on-demand data using sophisticated intuitive queries increases dramatically. This research presents a cloud-centric vision for the global implementation of Internet of Things. The main enabling technologies and areas of application likely to drive IoT research in the near future are discussed. A cloud implementation using Aneka, based on the interaction of private and public clouds, is presented. The authors conclude our IoT vision by developing the need for convergence of WSN, Internet and distributed computing directed towards the technology research community. The proliferation of devices with communication actuation capabilities brings Internet vision closer to things, where detection and actuation functions blend perfectly in the background and new functionality is made possible by access to New sources of rich information. The evolution of the next generation mobile system will depend on the creativity of users in designing new applications. IoT is an emerging technology ideal for influencing this field by providing new scalable data and IT resources required to create revolutionary applications. Presented here, there is a user-centric cloud-based model to address this goal through the interaction of private and public clouds. In this way, the needs of the end user are highlighted. Given the flexibility to meet the diverse and sometimes competing needs of different sectors, the authors propose a framework for an evolutive cloud to provide the capacity to use IoT. The framework makes it possible to separate the themes of networking, computing and storage and visualization, which allows independent growth in all sectors but complement each other in a shared environment. The normalization that takes place in each of these themes will not be affected by Cloud in its center. In proposing the new framework, the associated challenges have been highlighted, ranging from appropriate interpretation and visualization of large amounts of data to privacy, security and data management issues that need to support such a platform, So that it is truly viable. The consolidation of international initiatives significantly accelerates progress towards an IOT, providing an overall view for integration and functional elements that can provide an operational IOT. [13].

3.2 Comparative Investigation on CSMA /CA-Based Opportunistic Random Access for Internet of Things

In 2014, Chong Tang, Lixing Song, Jagadeesh Balasubramani, Shaoen Wu, Saâd Biaz, Qing Yang, and Honggang Wang presents there paper **"Comparative Investigation on CSMA/CA-Based Opportunistic Random Access for Internet of Things"**. According to their work Wireless communication is indispensable to Internet of Things (IoT). Carrier sensing multiple access/collision avoidance (CSMA/CA) is a well-proven wireless random access protocol and allows each node of equal probability in accessing wireless channel, which incurs equal throughput in long term regardless of the channel conditions. To exploit node diversity that refers to the difference of channel condition among nodes, this paper proposes two opportunistic random access mechanisms: overlapped contention and segmented contention, to favor the node of the best channel condition. In the overlapped contention, the contention windows of all nodes share the same ground of zero, but have different upper bounds upon channel condition. In the segmented contention, the contention window upper bound of a better channel condition is smaller than the lower bound of a worse channel condition; namely, their contention windows are segmented without any overlapping. These algorithms are also polished to provide temporal fairness and avoid starving the nodes of poor channel conditions. The proposed mechanisms are analyzed, implemented, and evaluated on a Linux-based test bed and in the NS3 simulator. Extensive comparative experiments show that both opportunistic solutions can significantly improve the network performance in throughput, delay, and jitter over the current CSMA/CA protocol. In particular, the overlapped contention scheme can offer 73.3% and 37.5% throughput improvements in the infrastructure-based and ad hoc networks, respectively. IoT requires effective medium access protocols for wireless communication. This work proposes two opportunistic random access variants to exploit node diversity in wireless networks. These algorithms enable nodes to access the shared wireless channel based on their channel conditions so that the node at the highest achievable bit rate is favored. To avoid starving nodes with poor channel conditions, a slow filtering scheme are proposed to maintain temporal fairness among nodes. With extensive experiments on a developed Linux-based test bed and the NS3 network simulator, the proposed opportunistic access schemes significantly improve the network performance in throughput, delay, and jitter, which can offer significant advantages for supporting future IoT applications.

3.3 Research Directions for the Internet of Things

The In 2014, John A. Stankovic presented his paper **"Research Directions for the Internet of Things".** According to his work many technical communities are vigorously pursuing research topics that contribute to the Internet of Things (IoT). Today, as sensing, actuation, communication, and control become ever more sophisticated and ubiquitous, there is significant overlap in these communities, sometimes from slightly different perspectives. More cooperation between communities is encouraged. To provide a basis for discussing open research problems in IoT, a vision for how IoT could change the world in the distant future is first presented. Then, eight key research topics are enumerated and research problems within those topics are discussed. IoT becomes a utility with increased sophistication in sensing, actuation, communications, control, and in creating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. What the lifestyles would be is anyone's guess. It would be fair to say that we cannot predict how lives will change. We did not predict the Internet, the Web, social networking, Face book, Twitter, millions of apps for smart phones, etc., and these have all qualitatively changed societies' lifestyle. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security. It is hoped that there is more cooperation between the research communities in order to solve the myriad of problems sooner as well as to avoid re-inventing the wheel when a particular community solves a problem.

3.4 WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings

For In 2015, Hemant Ghayvat, Subhas Mukhopadhyay, Xiang Gui and Nagender Suryadevara proposed their paper **"WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings".** Their research approach is to design and develop reliable, efficient, flexible, economical, real-time and realistic wellness sensor networks for smart home systems.

The heterogeneous sensor and actuator nodes based on wireless networking technologies are deployed into the home environment. These nodes generate real-time data related to the object usage and movement inside the home, to forecast the wellness of an individual. Here, wellness stands for how efficiently someone stays fit in the home environment and performs his or her daily routine in order to live a long and healthy life. We initiate the research with the development of the smart home approach and implement it in different home conditions (different houses) to monitor the activity of an inhabitant for wellness detection. Additionally, our research extends the smart home system to smart buildings and models the design issues related to the smart building environment; these design issues are linked with system performance and reliability. This research paper also discusses and illustrates the possible mitigation to handle the ISM band interference and attenuation losses without compromising optimum system performance.

4. IOT TECHNOLOGIES

The Internet of Things [15] was initially inspired by members of the RFID community, who referred to the possibility of discovering information about a tagged object by browsing an internet address or database entry that corresponds to a particular RFID or Near Field Communication [16] technologies. In the research paper "Research and application on the smart home based on component technologies and Internet of Things", the included key technologies of IoT are RFID, the sensor technology, nano technology and intelligence embedded technology. Among them, RFID is the foundation and networking core of the construction of Internet of Things [17]. The Internet of Things (IoT) enabled users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like NFC, RFID and 2D barcode which allowed physical objects to be identified and referred over the internet [18]. IoT, which is integrated with Sensor Technology and Radio Frequency Technology, is the ubiquitous network based on the omnipresent hardware resources of Internet, is the Internet contents objects together. It is also a new wave of IT industry since the application of computing fields, communication network and global roaming technology had been applied. It involves in addition to sophisticated technologies of computer and communication network outside, still including many new supporting technologies of Internet of Things, such as collecting Information Technology, Remote Communication Technology, Remote Information Transmission Technology, Sea Measures Information Intelligence Analyzes and Controlling Technology etc. [19].

4.1 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a system that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number [20]. First use of RFID device was happened in 2nd world war in Brittan and it is used for Identify of Friend or Foe in 1948. Later RFID technology is founded at Auto-ID center in MIT in the year 1999. RFID technology plays an important role in IoT for solving identification issues of objects around us in a cost effective manner [5]. The technology is classified into three categories based on the method of power supply provision in Tags: Active RFID, Passive RFID and Semi Passive RFID. The main components of RFID are tag, reader, antenna, access controller, software and server. It is more reliable, efficient, secured, inexpensive and accurate. RFID has an extensive range of wireless applications such as distribution, tracing, patient monitoring, military apps etc. [21].

4.2 Internet Protocol (IP)

Internet Protocol (IP) is the primary network protocol used on the Internet, developed in 1970s. IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6. Each version defines an IP address differently. Because of its prevalence, the generic term IP address typically still refers to the addresses defined by IPv4. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. The actual protocol provides for 4.3 billion IPv4 addresses while the IPv6 will significantly augment the availability to 85,000 trillion addresses [22]. IPv6 is the 21st century Internet Protocol. This supports around for 2128 addresses.

4.3 Electronic Product Code (EPC)

Internet Electronic Product Code (EPC) is a 64 bit or 98 bit code electronically recorded on an RFID tag and intended to design an improvement in the EPC barcode system. EPC code can store information about the type of EPC, unique serial number of product, its specifications, manufacturer information etc. EPC was developed by Auto-ID center in MIT in 1999. EPCglobal Organization [Wikipedia, "EPCglobal", 2010] which is responsible for standardization of Electronic Product Code (EPC) technology, created EPCglobal Network [Wikipedia, "EPCglobal Network", 2010] for sharing RFID information. It has four components namely Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS) and EPC Security Services (EPCSS).

4.4 Barcode

Barcode is just a different way of encoding numbers and letters by using combination of bars and spaces of varying width. Behind Bars [23] serves its original intent to be descriptive but is not critical. In The Bar Code Book, Palmer (1995) acknowledges that there are alternative methods of data entry techniques. Quick Response (QR) Codes the trademark for a type of matrix barcode first designed for the automotive industry in Japan. Bar codes are optical machine-readable labels attached to items that record information related to the item. Recently, the QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard. There are 3 types of barcodes of Alpha Numeric, Numeric and 2 Dimensional. Barcodes are designed to be machine readable. Usually they are read by laser scanners, they can also be read using a cameras.

4.5 Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. Vic Hayes has been named as father of Wireless Fidelity. The precursor to Wi-Fi was invented in 1991 by NCR Corporation in Nieuwege in the Netherland. The first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbps to 2 Mbps. Today, there are nearly pervasive Wi-Fi that delivers the high speed Wireless Local Area Network (WLAN) connectivity to millions of offices, homes, and public locations such as hotels, cafes, and airports. The integration of Wi-Fi into notebooks, handhelds and Consumer Electronics (CE) devices has accelerated the adoption of Wi-Fi to the point where it is nearly a default in these devices [24]. Technology contains any type of WLAN product support any of the IEEE 802.11 together with dual-band, 802.11a, 802.11b, 802.11g and

802.11n. Nowadays entire cities are becoming Wi-Fi corridors through wireless APs.

4.6 Bluetooth

Bluetooth wireless technology is an inexpensive, short-range radio technology that eliminates the need for proprietary cabling between devices such as notebook PCs, handheld PCs, PDAs, cameras, and printers and effective range of 10 - 100 meters. And generally communicate at less than 1 Mbps and Bluetooth uses specification of IEEE 802.15.1 standard. At first in 1994 Ericson Mobile Communication company started project named "Bluetooth". It is used for creation of Personal Area Networks (PAN). A set of Bluetooth devices sharing a common channel for communication is called Piconet. This Piconet is capable of 2 - 8 devices at a time for data sharing, and that data may be text, picture, video and sound. The Bluetooth Special Interest Group comprises more than 1000 companies with Intel, Cisco, HP, Aruba, Intel, Ericson, IBM, Motorola and Toshiba.

4.7 ZigBee

ZigBee is one of the protocols developed for enhancing the features of wireless sensor networks. ZigBee technology is created by the ZigBee Alliance which is founded in the year 2001. Characteristics of ZigBee are low cost, low data rate, relatively short transmission range, scalability, reliability, flexible protocol design. It is a low power wireless network protocol based on the IEEE 802.15.4 standard [25]. ZigBee has range of around 100 meters and a bandwidth of 250 kbps and the topologies that it works are star, cluster tree and mesh. It is widely used in home automation, digital agriculture, industrial controls, medical monitoring & power systems.

4.8 Near Filed Communication (NFC)

Near Field Communication (NFC) is a set of short-range wireless technology at 13.56 MHz, typically requiring a distance of 4 cm. NFC technology makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch. Allows intuitive initialization of wireless networks and NFC is complementary to Bluetooth and 802.11 with their long distance capabilities at a distance circa up to 10 cm. It also works in dirty environment, does not require line of sight, easy and simple connection method. It is first developed by Philips and Sony companies. Data exchange rate now days approximately 424 kbps. Power consumption during data reading in NFC is under 15ma.

4.9 Actuators

An actuator is something that converts energy into motion, which means actuators drive motions into mechanical systems. It takes hydraulic fluid, electric current or some other source of power. Actuators can create a linear motion, rotary motion or oscillatory motion. Cover short distances, typically up to 30 feet and generally communicate at less than 1 Mbps. Actuators typically are used in manufacturing or industrial applications. There are three types of actuators are (1) Electrical: ac and dc motors, stepper motors, solenoids (2) Hydraulic: use hydraulic fluid to actuate motion (3) Pneumatic: use compressed air to actuate motion. All these three types of actuators are very much in use today. Among these, electric actuators are the most commonly used type. Hydraulic and pneumatic systems allow for increased force and torque from smaller motor.

4.10 Wireless Sensor Networks (WSN)

A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations (Wikipedia). Formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another. A wireless sensor network is an important element in IoT paradigm. Sensor nodes may not have global ID because of the large amount of overhead and large number of sensors. WSN based on IoT has received remarkable attention in many areas, such as military, homeland security, healthcare, precision agriculture monitoring, manufacturing, habitat monitoring, forest fire and flood detection and so on [26]. Sensors mounted to a patient's body are monitoring the responses to the medication, so that doctors can measure the effects of the medicines [27].

4.11 Artificial Intelligence (AI)

Artificial Intelligence refers to electronic environments that are sensitive and responsive to the presence of people. In an ambient intelligence world, devices work in concert to support people in carrying out their everyday life activities in easy, natural way using Information and Intelligence that is hidden in the network connected devices. It is characterized by the following systems of characteristics (1) Embedded: Many Net- worked devices are integrated in to the environment (2) Context Aware: These devices can recognize you and your situational context (3) Personalized: They can be tailored to your needs (4) Adaptive: They can change in response to you (5) Anticipatory: They can anticipate your desires without conscious mediation.

5. CONCLUSION

After In this survey paper proposed the bird eye view on different type of IOT, also represent the different IOT techniques used in previous research. Now a days IOT and its different type is burning topic in between researcher. In this paper shows the main technical issue of IOT and also describe the technical challenges in the IOT establishment. After the discussion of technical problem focus on the main technology of IOT used. At the last shows the review of different previous papers of different researchers.

6. REFERENCES

[1] Bowman, Lianos, M. and Douglas, M. (2000) Dangerization and the End of Deviance: The Institutional Environment. *British Journal of Criminology*, **40**, 261-278.

[2] Ferguson, T. (2002) Have Your Objects Call My Object. *Harvard Business Review*, June, 1-7.

[3] Nunberg, G. (2012) The Advent of the Internet: 12th April, Courses.

[4] Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. *Advances in Internet of Things*: *Scientific Research*, **1**, 5-12.

[5] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". *First International Conference on Security of Internet of Things*, Kerala, 17-19 August 2012, 51-56.

[6] Biddlecombe, E. (2009) UN Predicts "Internet of Things". Retrieved July 6.

[7] Butler, D. (2020) Computing: Everything, Everywhere. *Nature*, **440**, 402-405.

[8] Dodson, S. (2008) The Net shapes up to Get Physical. Guardian.

[9] Gershenfeld, N., Krikorian, R. and Cohen, D. (2004) the Internet of Things. *Scientific American*, **291**, 76-81.

[10] Lombreglia, R. (2010) the Internet of Things, Boston Globe. Retrieved October.

[11] Reinhardt, A. (2004) A Machine-to-Machine Internet of Things.

[12] Graham, M. and Haarstad, H. (2011) Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things. *Research Article*, **7**.

[13] Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. Future Generation.

[14] Gigli, M. and Koo, S. (2011) Internet of Things, Services and Applications Categorization. *Advances in Internet of Things*, **1**, 27-31. http://dx.doi.org/10.4236/ait.2011.12004

[15] (2005) ITU Internet Reports, International Telecommunication Union. The Internet of Things: 7th Edition. www.itu.int/internetofthings/on

[16] Want, R. (2006) An Introduction to RFID Technology. *IEEE Pervasive Computing*, **5**, 25-33.

[17] Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internet of Things. *Procedia Engineering*, **15**, 2087-2092. http://dx.doi.org/10.1016/j.proeng.2011.08.390

[18] Razzak, F. (2012) Spamming the Internet of Things: A Possibility and its probable Solution. *Procedia Computer Science*, **10**, 658-665. http://dx.doi.org/10.1016/j.procs.2012.06.084

[19] Shao, W. and Li, L. (2009) Analysis of the Development Route of IoT in China. *Perking*: *China Science and Technology Information*, **24**, 330-331.

[20] Sun, C. (2012) Application of RFID Technology for Logistics on Internet of Things.

[21] Moeinfar, D., Shamsi, H. and Nafar, F. (2012) Design and Implementation of a Low-Power Active RFID for Container Tracking @ 2.4 GHz Frequency: Scientific Research.

[22] Bicknell, IPv6 Internet Broken, Verizon Route Prefix Length Policy, 2009.

[23] Grieco A., Occhipinti, E. and Colombini, D. (1989) Work Postures and Musculo-Skeletal Disorder in VDT Operators. *Bollettino de Oculistica*, Suppl. 7, 99-111.

[24] Pahlavan, K., Krishnamurthy, P., Hatami, A., Ylianttila, M., Makela, J.P., Pichna, R. and Vallstron, J. (2007) Handoff in Hybrid Mobile Data Networks. *Mobile and Wireless Communication Summit*, **7**, 43-47.

[25] Chen, X.-Y. and Jin, Z.-G. (2012) Research on Key Technology and Applications for the Internet of Things. *Physics Procedia*, **33**,561-566. http://dx.doi.org/10.1016/j.phpro.2012.05.104

[26] Arampatzis, T., *et al*. (2005) A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control. *Proceeding of the IEEE International Symposium on, Mediterrean Conference on Control and Automation*, 719-724.

[27] Chorost, M. (2008) The Networked Pill, MIT Technology Review, March.