General Survey on Security Issues on Internet of Things

Dolly Das
Department of CSE & IT
School of Technology
Assam Don Bosco University

Bobby Sharma
Department of CSE & IT
School of Technology
Assam Don Bosco University

ABSTRACT
Internet of Things is the integration of a variety of technologies. The Internet of Things incorporates transparently and impeccably large number of assorted end systems, providing open access to selected data for digital services. Internet of things is a promising research in commerce, industry, and education applications. The abundance of sensors and actuators motivates sensing and actuate devices in communication scenarios thus enabling sharing of information in Internet of Things. Advances in sensor data collection technology and Radio Frequency Identification technology has led large number of smart devices connected to the Internet, continuously transmitting data over time.In the context of security, due to different communication overloads and standards conventional security services are not applicable on Internet of Things as a result of which the technological loopholes leads to the generation of malicious data, devices are compromised and so on. Hence a flexible mechanism can deal with the security threats in the dynamic environment of Internet of Things and continuous researches and new ideas needs to be regulated periodically for various upcoming challenges. This paper basically tries to cover up the security issues and challenges of Internet of Things along with a brief introduction on Internet of Things, its elements and components such as Radio Frequency Identification, Wireless Sensor Network and Near Field Communication.

General Terms
Ad Hoc Network, Sensors, Actuators, Ubiquitous Computing, Security, Privacy, Confidentiality.

Keywords
Internet of Things, Machine-to-machine Communication, Vehicle-to-vehicle Communication, Security Issues, Secure Reprogrammable Networks.

1. INTRODUCTION
Today, Communication is enveloping as there is a growing interest in sharing data through the Internet. The emergence of objects like sensors has been able to adapt and build a firm connection through the Internet in comparison to the conventional objects in use. Thus the evolution of advanced wireless technology envisioning a tomorrow, with objects equipped with microcontrollers, transceivers and protocol stacks making communication easier with the users, enables Internet of Things, to reach a remarkable position today. Objects such as Radio Frequency Identification, Near Field Communication, sensors, actuators, mobile phones are able to interact through unique addressing schemes through the modern concept of Internet of Things. The most obvious impact can be observed in domestic sphere-assisted living, the potential area increasing the living standard of an entity. In business, Internet of Things can be realized in production, superior quality etc. The main setback of Internet of Things is security with problems like addressing problem, scalability problem, etc. Internet of Things is using limited traffic without demanding tremendous revenues to operators for traffic sale. The growing computation power in objects shifts services remote of the network thus decreasing their revenues.

2. INTERNET OF THINGS
2.1 Invention and Conception
The name Internet of Things coined by Kevin Ashton originated in the Auto-ID Centre at Massachusetts Institute of Technology in 1999[1,5] with the aim of making an object sense information without human intervention.

The entire concept of Internet of Things is about the achievement of persistent connections between the Internet and objects . Here, connections will proliferate and create an entirely new vibrant network of networks. It is based on technical advances and visions of network ubiquity being realized. It aims at making the Internet more enveloping, cultivating the development of applications of potential data to provide new services[3]. The main ideology behind this concept is the ability to connect loosely defined smart objects enabling them to connect with other objects, the environment or more complex legacy computing devices.

Internet of Things has been made applicable to evolving intelligent frameworks in industry, agriculture, logistics, transportation, smart lattice, environmental shield, security fortification, medical care, smart home, and smart cities[3].To establish a smart connection and a context-aware computation Internet of Things demands three fundamental grounds - mutual understanding of the state of affairs of users and their appliances, software design and pervasive communication topologies to process and convey the appropriate information and self-governing and smart performance.

2.2 Definition
According to Atzori et al. [8], Internet of Things can be realized in three paradigms namely semantic-oriented ,Internet-oriented and things-oriented .The effectiveness of Internet of Things can be unleashed in an application domain where the three paradigms intersect.[5]

2.3 Elements
A taxonomy aids in defining the components from a high level perception. There are three Internet of Things components[6,12] which enables flawless Ubiquitous Computing-hardware ,middleware and presentation.

The Internet of Things infrastructure makes use of TCP or UDP protocols as a transmission protocol for the transmission of data. TCP has some challenges such as connection setup, congestion control, and data buffering. Quality of Service in the Internet of Things systems can be executed on the communication localized on Wireless Sensor Network with different paradigms, characteristic and behavior. The most important factor in the Internet of Things is to build a standard

and universal architecture as it is an abode of different targets, applications, and features. Internet of things can be applied in diverse fields like in Transportation and logistics domain such as smart parking, 3D assisted driving, in healthcare domain, in smart environments domain such as smart homes and offices etc.

2.4 Radio Frequency Identification

Radio Frequency Identification [1,9,10,13] system is composed of readers and several Radio Frequency Identification tags with a specific address. Tags make use of radio frequency induced electromagnetic fields to transfer data attached to an object. The electronic information in the tags are read by the Radio Frequency Identification reader when the object comes in the proximity of the reader. Radio Frequency Identification as shown in Figure 1[19] monitors objects in real-time, without being in line-of-sight. Radio Frequency Identification tag is a infinitesimal microchip pooled with an antenna in a compact pack up. Hitachi has developed a tag with dimensions 0.4*0.4*0.15 mm. In Internet of Things hosts are addressed i.e. the readers are the hosts in the network and devices are named i.e. the Radio Frequency Identification tags are the devices. Hosts need to be reachable and posses routing capabilities via the Domain Name System (DNS) or using the Border Gateway Protocol(BGP).

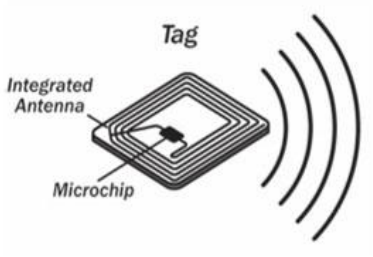

Fig 1: Radio Frequency Identification Tag

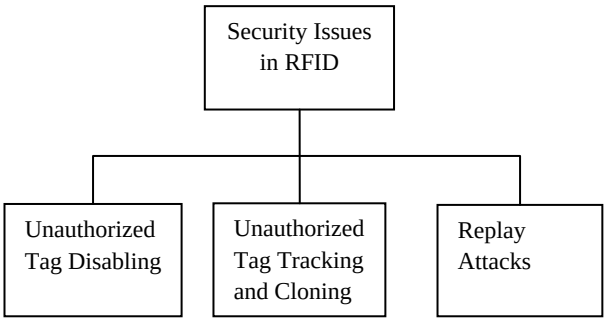

Fig 2: Security Issues in Radio Frequency Identification

Table 1. Classification of Radio Frequency Identification Tags

Items	Passive Radio Frequency Identification tag	Active Radio Frequency Identification tag	Active Radio Frequency Identification tag(new)
Communication Range	70cm/3m-7m	More than 10m	10m
Battery Life	No battery	Around 1 year	1 year
Security	Weak	NA/ Weak	Strong
Cost	Less than $1	Less than $10	Around $10
Application	Distribution/inventory controls of goods	Tracking person(restricted area)	Tracking person(no restriction)

2.5 Near Field Communication

Near Field Communication (NFC) is an integration of Radio Frequency Identification reader in a mobile phone in a customer-oriented fashion as shown in Figure 3[20]. Near Field Communication operates within the unlicensed Radio Frequency band of 13.56 MHz; the typical operating range of Near Field Communication device is 20 cm. The operating range is depended on the size of the antenna. Near Field Communication enabled communication between the smart objects is safe because it cannot be done from a remote location. The Near Field Communication[1] technology will significantly contribute to the future development of Internet of Things facilitating the necessary tool to be wirelessly associated to any smart objects. Mobile Near Field Communication also has the potential to renovate the mobile headsets into dissimilar types of smart objects for eg. when we need to pay the bills our mobile can be used as our credit card.

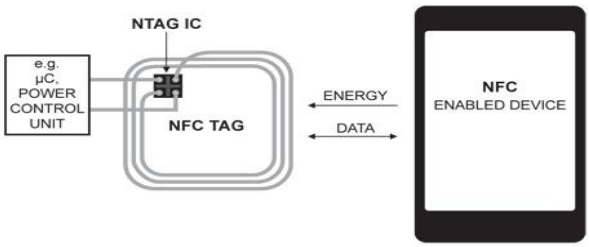

Fig 3: Near Field Communication

2.6 Machine-to-machine Communication

Machine-to-Machine (M2M) is the communication amid computers, entrenched processors, elegant sensors, actuators and mobile devices. In [1,2,16] Machine-to-Machine Communication refers to the interconnection established and interoperability between various machines, achieved by data swap through wireless transmission and backend content servers, without human intervention. The four components of Machine-to-machine communication - sensing, varied access, information dispensation, application and services allows organizations perform relevant work, develop standards, like the 3rd Generation Partnership Project (3GPP).From the technical point of view, Machine-to-machine communication is a five-part structure as shown in Figure 5[2].

1. M2M Device replies to request for data enclosed within that device.
2. M2M Area Network provides connectivity between M2M Devices and Gateways.
3. M2M Gateway uses M2M capabilities to ensure M2M Devices interacting to the communication entity.

4. M2M Communication Network between the M2M Gateways and application.

Today, 3G and 4G wireless technologies play an important role by high calibre of their higher data transmission tariff, satisfying the requirements of more M2M application services realized in cellular networks specially those which are mobile, Wireless Local Area Networks and Wireless Sensor Networks.

2.7 Wireless Sensor Network

A Wireless Sensor Network is a self-organizing sensor network with nodes deployed in liberated space in a prearranged distribution [4,9,13]. The sensors complete monitoring the environmental conditions such as temperature, humidity, chemical symphony, pressure, resonance, displacement, pulsation and contaminated particles and understand the given conditions and enable applications to make automatable decisions through specified rules.

2.8 Vehicle-to-vehicle Communication

Vehicle-to-Vehicle Communication is a new concept where vehicles acts as nodes and communicate with every other by employing sensors allied in an extemporized network within a range of 1000m. Two types of communication are possible: vehicle-to-vehicle and road-side vehicle communications. Vehicular communication system is built-up as a part of the Intelligent Transport System (ITS).

2.9 Internet of Things Devices

The devices that are essential to realize an urban Internet of Things[3,14], classified based on the position they occupy in the communication flow are:

2.9.1. Backend Servers

Found at the root of the system, located in the control centre, where data are collected, stored, and processed to produce added-value services. Backend systems interface with the Internet of Things database management systems, websites and enterprise resource planning systems. A database management system stores the outsized sum of information formed by Internet of Things tangential nodes, such as sensors. Websites enables interoperation between the Internet of Things system and the data consumers. Enterprise Resource Planning systems (ERP) are precious tools to manage the flow of information.

2.9.2. Gateways

Gateways interconnect the end devices to the main communication infrastructure of the system thus providing protocol conversion and well-designed mapping amid the dumped protocols and their subdued counterparts.

2.9.3. Internet of Things Peripheral Nodes

These devices produce data to be delivered to the control centre; may be off the record based on powering mode, networking role, sensor/actuator equipment and link layer technologies.

3. LITERATURE SURVEY

In [1],the authors have presented Internet of Things in a wider context . The paper describes the key technologies involved in its implementation and the major application domain where Internet of Things will play a vital role. It discusses the open issues of these technologies.

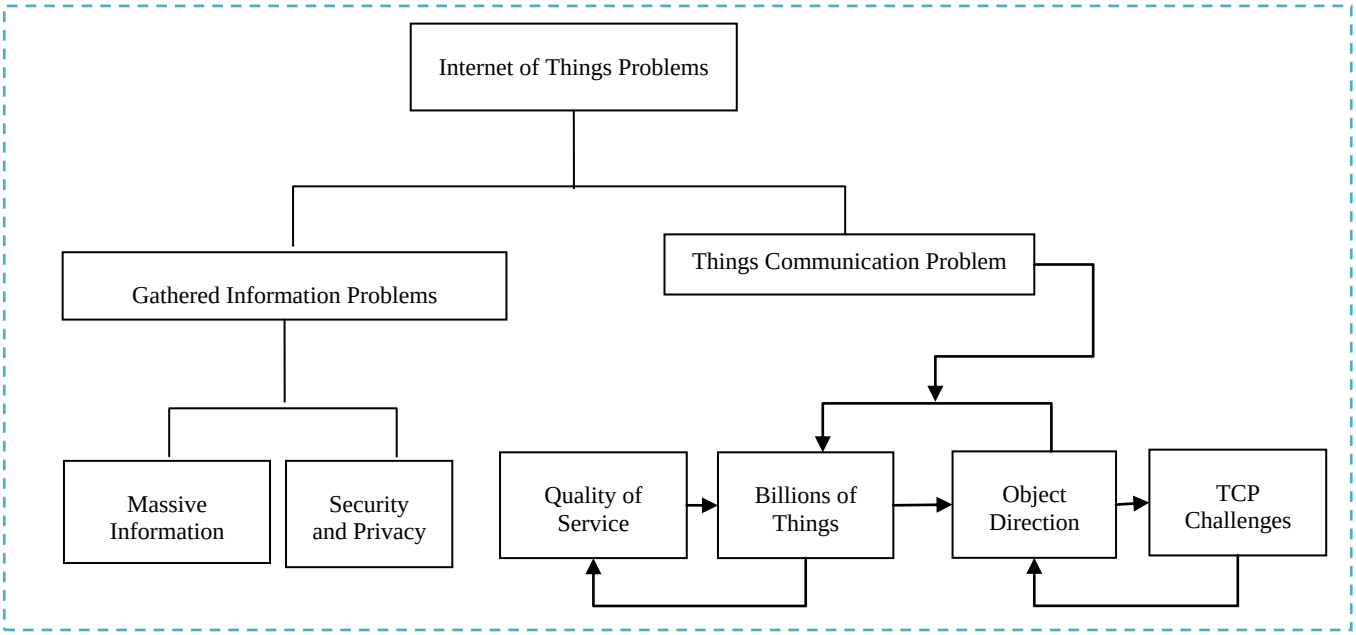

Fig 4: Internet of Things Problems

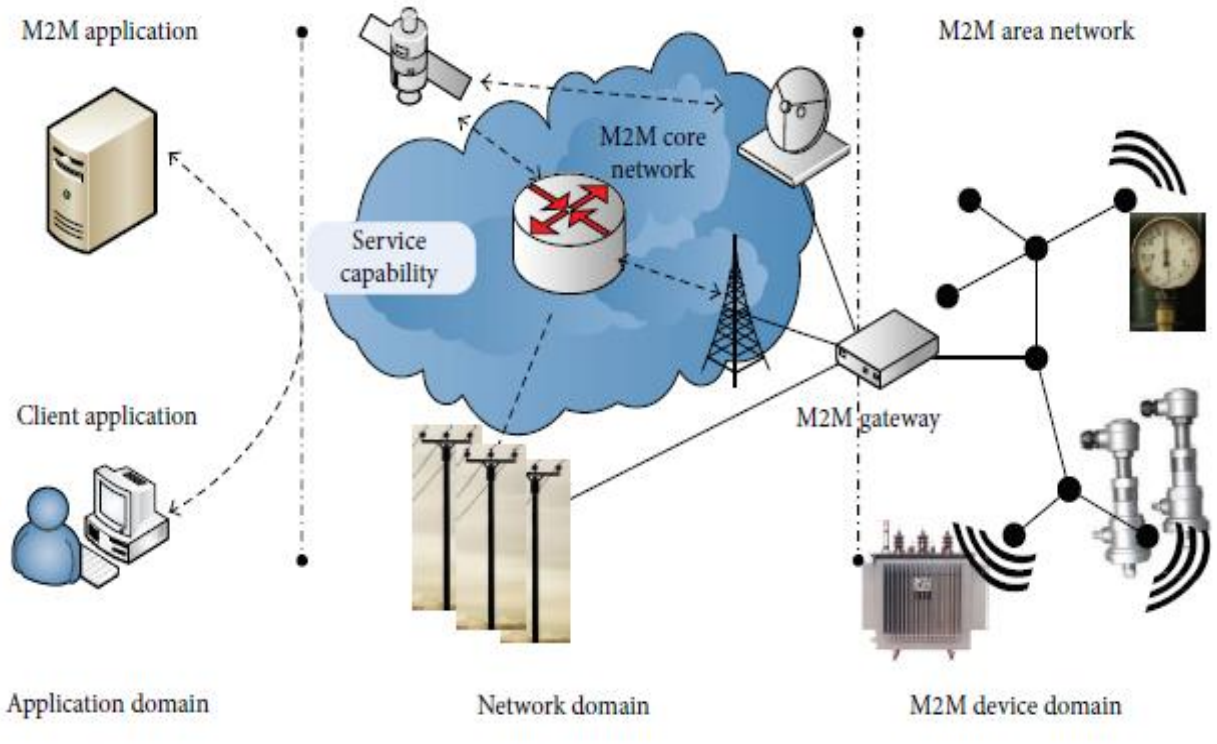

Fig 5: Machine-to-machine Communication

In [2] the paper suggests topics as routing, networking, and data mining, setting new research angles regarding the Internet of Things serving a key purpose from the standpoint of correlative technology based on time, to reconsider the evolutionary course of action of the Internet of Things and portray the relationships between the correlation techniques largely missing in the current works carried out on Internet of Things.

From [3], we have their focus specifically on urban Internet of Things system based on the application domain. Urban Internet of Things supports the Smart City apparition, exploiting the refined technologies to prop up added-value services for the supervision of the city and its citizens. The authors provide a all-inclusive survey of the urban Internet of Things. Additionally, they have presented and discussed the Padova Smart City project, deploying Internet of Things.

In [4], the history of Internet of things, different proposed architectures of Internet of things, delves into challenges and inconvenience related to the Internet of things has been discussed by the authors.

In [5] the authors have presented the various research challenges, some open issues are discovered and hints for further research direction are advocated.

Data Center Trends discussed at the Gartner Infrastructure, Operations and Data Center Summit on 21-22 May of 2014 in Sydney stated that by 2020 the Internet of Things shall include 26 Billion Units. The Internet of Things (IoT) has a probable transformational cause on the data center market, its customers, technology providers and sales and marketing models. The incremental revenue shall exceed $300 billion, mostly in services. Research Director Fabrizio Biscotti in Gartner stated that Internet of Things deployments will generate challenges towards big data in security, capacity and analytics.

4. ANALYSIS OF SECURITY ISSUES

4.1.Internet of Things Security Requirement

Firstly, sensor security, including sensor meddling, safeguarded, signal intercepted and secondly the normal operation of the sensor, transmission and treatment systems are a must for Internet of Things. Thirdly data security, that demands, the information in the sensor, the transmission system and the processing system shall be assured of not being stolen, tampered, forged or denied.

4.2. Information Gathering Problems

As shown in Figure 4[4] these problems can be divided to two main classes- massive information gathered by Radio Frequency Identification about huge number of things found at Internet of Things system and the security and the privacy of information due to wireless transmission media.

4.2.1. Massive gathered information

The Internet of Things systems should have millions of objects that emanate information to express itself [4] that leads to transmission, storing, and processing problems. Transmission of all things data in real time is not guaranteed because of the bandwidth bottlenecks; data storing is raised due to the quantity of media required to store and backup the information; processing becomes slow due to such overheads. The Internet of Things gathered information can be classified into- Radio Frequency Identification data stream, Address/unique identifiers, Descriptive data, Positional data, Environment data , sensor network data etc.

The Internet of Things system produces throng information. Radio Frequency Identification needs approximately 18 bytes of raw data for such information, hence the necessity to find effectual methods for storing, filtering and modifying Radio Frequency Identification raw data arises. The special

characteristics of Internet of Things such as mass data, distributed data, time-related data, and heterogeneous environment convey numerous problems to centralized data mining architecture.

4.2.2. Security and privacy

In a wireless medium the security and privacy issues are important as the threats to the Internet of Things[14,15] information are more such as physical attack, wireless information attack, snooping and low self-defence. Hacker might tamper the unattended Internet of Things devices and can acquire the information before it is inward by the destination. In low self defence, Internet of Things devices lose the ability to accept security package(s) for partial safety.

The major problems with Internet of Things[7] are security concern, authentication and data integrity with the increase in the number of such smart objects in the wireless network. Solutions like Keyed-Hash Message Authentication Code (HMAC) scheme, to protect the data against the attack have been proposed. However, new researches are still required in the field of security and privacy.

Since security is a crucial component to enable the extensive adoption of Internet of Things technologies and applications. Thus without system-level confidentiality, authentication and privacy, the related stakeholders are unlikely to go for Internet of Things solutions on a large scale. Hence, without proper inventions and discovery of innovative security measures and new research works it seems the legacy of threats and being compromised is likely to get continued.

Privacy on the other hand enables information provider to infer by observing the utilization of the system related to each system client such that inference should be very hard to carry out. The personal data collected should be used by authorized person, stored in an authorized server, and accessed by authorized clients. The security and privacy needs three main requirements such as pliability to attack, data authentication and client privacy.

4.3.Data confidentiality

Data confidentiality in Internet of Things[7] is a primary constraint that guarantees access and modification to certified entities via an access control mechanism and object authentication practice with a related identity supervision system. Various research challenges such as defining mechanisms for domineering access to data streams generated in Internet of Things, implementing manipulation language for enabling applications to salvage the desired information from the stream of data and by defining certain smart objects identity management system can help in ensuring data confidentiality.

4.4.Trust

Trust conciliation refers to the procedure of credential exchanges that allows a party needing a service or a resource from another party to provide the necessary permit to obtain the service or the resource. Trust intercession relies on end-to-end communications and consists iterative revelation of digital credentials, authorized by given entities, for verifying attributes of their holders to ascertain mutual trust. A trust arbitration system exploits digital characteristics information to provide a fine-grained access manage to cosseted resources. The capability to meet the trust constraint is indeed strictly correlated to the distinctiveness management and access control issues.

Many open issues have to be addressed[5] in order to develop Internet of Things trust services such as effective trust negotiation language , effective distributed model of trust and a new flexible framework for trust management

4.5. Access Control

Access control[7] deals with access rights given to the things and devices in Internet of Things environment. Data holders and data collectors supervise and manage the access control in Internet of Things. A few of the challenges related in Internet of Things[4,12] perspective such as how to handle the huge amount of transmitted data in a common recognized representation or how to support the identification of entities.

4.6.Policy Enforcement

It implies to the approach that causes the application of a set of definite efforts in a system. Policies[5] are performing rules desired for acknowledging order, security, and consistency on data. It is necessary to detect the enforcement mechanism acceptable for the definite Internet of Things[11] framework, locating symmetry between the assertion of security and privacy issues, demand of computing efforts by the steadfast mechanisms.

4.7. Mobile Security

Internet of Things constitutes of mobile nodes that moves from one cluster to another where cryptanalysis protocols allow prompt identification, authentication, and privacy protection. It will safeguard against replay attack, eavesdropping etc. In contrast with protocols such as basic hash protocol, an ad hoc protocol has less communication overheads, more security and provides privacy protection. With respect to the security issues of mobile devices, under research by the scientific community, the available solutions fairly address these needs, requiring further efforts to allow the amalgamation with the other Internet of Things technologies.

4.8. Secure Middleware

Numerous types of middleware layer effects the incorporation and the security of devices and data within the indistinguishable information network. In middleware design and development, data needs to have exact protection constraints, different communication mediums for wide scale deployments of Internet of Things. Ad hoc gateways along with middleware, adapts to differing to all the Internet of Things conditions, coupled in terms of security, privacy and network behaviour.

4.9. Secure Reprogrammable Networks

There are many ways the system could be attacked, wherever networks are deployed at large scale such as disabling network availability, generating malicious data, accessing private information etc. The components of Internet of Things are vulnerable to attacks. Intermittently, new sensor applications need to be installed or existing ones need to be updated by isolated wireless reprogramming of the entire nodes in the network. Conventional network reprogramming is a security threat. A protected reprogramming practice allows the nodes to approve every code revise and prevent malicious installation.

4.10. Identification

Each object should be specific. Depending on the explicit state of affairs, objects should be exclusively recognized as belonging to a given class through Radio Frequency Identification tags or objects' depiction in wireless means.

4.11. Security Management

Security management can be carried out by identifying a person or object in motion called tracking or by identification and authentication. Sensing privacy in data sharing and management by maintaining information person-centric also helps in dealing with security management. Data collection can also help by reducing form processing time[8], process mechanization etc.

5. SECURITY CHALLENGES IN INTERNET OF THINGS

Majority of the devices in Internet of Things are not reachable as most of the time devices remain disconnected or loses connection. They could be lost or stolen thus making security very difficult. Expectation of strong security is difficult without processing power. As most of the devices are sensors and depends on battery life, devices maintain a finite lifetime. Devices are transportable and mostly mobile and should be recognised by readers based on Radio Frequency Identification addresses or tags along with proper authentication and device identification. Security works on Internet of Things must include assurance of risk analysis, device analysis, crypto capability and export analysis and must fulfil certain security objectives such as privacy protection, identity protection and traffic analysis protection.

Security in Internet of Things is mainly depended on the capability of the users to have faith in their environment. It is the top priority of the sector. Poorly secured Internet of Things devices could serve as ingress points for cyber attack by allowing malicious programmers to re-program a device or cause it to perform a malfunction intentionally. Poorly designed devices can expose user data to theft by leaving data streams and objects unattended. Competitive cost and technical constraints on Internet of Things devices challenge manufacturers to reasonably design security characteristics into these devices, potentially creating safety measures and enduring maintainability vulnerabilities greater than their traditional computer counterparts. The sheer increase in the number and nature of Internet of Things devices could increase the attacks. When united with the extremely interconnected character of Internet of Things devices, every poorly secured device linked online affects the security and flexibility of the Internet.

The increasing level of dependence on Internet of Things devices and the Internet services they interact with also enhances the pathways for wrongdoers to have access to devices and get compromised as their behavior has a global reach and impact. Turning off the devices is not an ideal solution at the same time for such issues. Thus security of Internet of Things devices and services is a critical issue.

The security of such devices is not absolute. The overall security and resilience of the Internet of Things is a utility of assessing and managing security risks. It is very important to understand the interrelatedness of Internet of Things in a wide manner.

Security Challenges:

1. Existing tools, methods, and strategies associated with Internet of Things security needs new consideration in comparison to the conventional system and strategies.
2. Deployment of homogenous Internet of Things may compromise its simplicity. Hopefully, a heterogeneous implementation strategy might work out properly.
3. Problems might arise in backgrounds like reconfiguration, evolution of the devices.
4. Long-term support and management of these devices
5. Improper knowledge regarding the device functionalities from the end users' part
6. Attackers may have direct physical access to Internet of Things devices. Anti-tamper features needs to be considered to ensure security in such cases
7. Security breach persists for long periods without detection
8. Future devices might be the products of various self manufacturers who finds themselves to be highly fascinated towards the technology in a similar manner today people are fascinated towards the development of enormous number of Android projects and devices of their own.
9. Shielding Programmable Logic Devices[18] from human interference
10. Maintenance of control systems for nuclear reactors receiving software updates periodically without impairing functional safety.

The effective and appropriate security solutions can be achieved only if the users involved with Internet of Things emerge with mutual security. The collaborative model emerges as an effective approach in industry, governments and public authorities to help secure the Internet, cyberspace and Internet of Things. This model includes a range of practices and tools including bidirectional voluntary information sharing, valuable enforcement equipments, cyber exercises, awareness raising and training, agreement on international norms of behaviour, and development and recognition of international standards and practices. However, collaborative and shared risk management-based approaches needs to keep on evolving such that it suits the scale and complexity of Internet of Things device security challenges of the future. Besides secure booting, access control, firewalls, IP address, device authentication, updates and patches, end-to-end security are also some of the solution to the security of Internet of Things[17].

6. CONCLUSION

This paper has tried to cover the entire concept of Internet of Things on security issues as far as possible based on various surveys and research works carried out so far and has tried to accomplish completeness -firstly with the introduction, its implementation, application, architecture, key components and elements, challenges, issues, security issues and threats, Internet of Things devices, security management, Quality of Services etc. The Internet of Things aims to effortlessly merge the real and implicit worlds such that tomorrow's globe will be a synthesis of human life and information. The current security services are inadequate for Internet of Things. The future research directions mainly consist of dealing with the development and challenges related to various issues on Internet of Things.

7. ACKNOWLEDGMENTS

I would like to thank Dr. Bobby Sharma, Assistant Professor, Department of Computer Science and Engineering and Information Technology, School of Technology, Assam Don Bosco University, for giving me the opportunity to perform a survey on security issues on Internet of Things, and providing

me to carry out an individual survey work in an efficient manner covering up all the necessary issues related to security of Internet of Things.

8. REFERENCES

[1] Shashank Agrawal and Dario Vieira. A Survey on Internet of Things. EFREI – Ecole d'ingénieur Informatique & technologies du numérique, France , VIT University, India . ABAKOS.

[2] Feng Wang, Liang Hu, Jin Zhou, and Kuo Zhao, "A Survey from the Perspective of Evolutionary Process in the Internet of Things", International Journal of Distributed Sensor Networks, February 2015, Hindawi Publishing Corporation

[3] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista and Michele Zorzi , "Internet of Things for Smart Cities*"* , IEEE Internet of Things Journal, Vol. 1, No. 1, February 2014.

[4] Omar Said and Mehedi Masud, "Towards Internet of Things: Survey and Future Vision", International Journal of Computer Networks (IJCN), Volume (5) , Issue (1), 2013.

[5] Ashvini Balte, Asmita Kashid and Balaji Patil, " Security Issues in Internet of Things(IoT): A Survey", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 4, 2015.

[6] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, Internet of Things(IoT): A vision, architectural elements and future directions. Future Generation Computer Systems. The University of Melbourne.

[7] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac. Internet of Things: Vision, Applications and Research Challenges. Ad hoc Networks. Università degli Studi dell' Italy.

[8] Luigi Atzori , Antonio Iera and Giacomo Morabito. The Internet of Things: A survey. Computer Networks. University of Cagliari, University Mediterranea of Reggio Calabria, University of Catania, Italy.

[9] Charu C. Aggarwal, Naveen Ashish and Amit Sheth. The Internet of Things: A Survey from the Data-Centric Perspective. IBM T.J.Watson Research Center, University of California , Wright State University.

[10] Sabita Maharjan, September 2010. RFID and IoT: An overview. Research Laboratory .University of Oslo.

[11] Isam Ishaq , David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman and Piet Demeester , "IETF Standardization in the Field of the Internet of Things(IoT):A Survey", Journal of Sensor and Actuator Networks,ISSN 2224-2708, April 2013.

[12] Min-Woo Ryu, Jaeho Kim, Sang-Shin Lee and Min-Hwan Song. Survey on Internet of Things: Toward Case Study. Smart Computing Review. Korea Electronics Technology Institute, vol.2, no. 3, June 2012.

[13] Prajakta Pande and Anand R. Padwalkar, "Internet of Things–A Future of Internet: A Survey", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 2, February 2014.

[14] Chen Qiang , Guang-ri Quan , Bai Yu and Liu Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking, Vol.6, No.6 , pp.1-10, 2013.

[15] Tuhin Borgohain, Uday Kumar and Sugata Sanyal. Survey of Security and Privacy Issues of Internet of Things. Assam Engineering College, Tech Mahindra Limited, India, Tata Consultancy Services, Mumbai, India.

[16] Manik Lal Das, Privacy and Security Challenges in Internet of Things

[17] https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

[18] http://pages.path.windriver.com/-WP-IoT-security-in-the-internet-of-things.

[19] https://www.google.co.in/imgres?imgurl=https://cdn.barcodesinc.com/cats/rfid-readers/tag.jpg&imgrefurl=https://www.barcodesinc.com/info/buying-guides/rfid.htm&h=186&w=277&tbnid=OF7idS3-BWPztM:&docid=ZtkKPoulHIn6yM&ei=i-zzVoLJLJaSuAS1u7yQAg&tbm=isch&ved=0ahUKEwjCupzht9nLAhUWCY4KHbUdDyIQMwiQAShYMFg

[20] https://www.google.co.in/search?q=NFC+IMAGES&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjJneX6ttnLAhUWkI4KHa-9ApEQ_AUIBygB&biw=1366&bih=649