International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

IOT Communication Technologies and Future of Internet of Things

Yeshwanth Valaboju[1]
[1]Consultant, VCERP Technologies Pvt. Ltd, India

ABSTRACT

The idea behind Internet of things is the interconnection of internet enabled things or devices to each other and to humans, to achieve some common goals. In near future IoT is expected to be seamlessly integrated into our environment and human will be wholly solely dependent on this technology for comfort and easy life style. Any security compromise of the system will directly affect human life.

Keywords : IoT, principles, IoT development, IoT security

I. INTRODUCTION

The concept of the Internet of Things (IoT) was introduced by Kevin Ashton, a co-founder of the Auto-ID Center at MIT, in 1998. The vision is that objects ("things") are connected to each other and thereby they create IoT in which each object has its distinct identity and can communicate with other objects. IoT objects can vary dramatically in size from a small wearable device to a cruise ship. IoT transforms ordinary products such as cars, buildings, and machines into smart, connected objects that can communicate with people, applications and each other.

There are various definitions of IoT. The International Telecommunication Union (ITU) defined the term Internet of Things as "Internet of Things will connect the world's objects in both a sensory and intelligent manner". In 2014, the Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) defined IoT as "an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react".3 At the IoT reception layer (Section 2.1.2), sensors placed within devices, objects, and machinery collect, measure, and record information about the physical environment, such as temperature, humidity, gas pressure, and motion. This information can be read, integrated and analyzed at higher IoT layers.

NIST uses two acronyms, IoT and NoT (Network of Things). IoT is considered a subset of NoT, since IoT has its "things" connected to the Internet. In contrast, some types of NoT use only Local Area Networks (LAN), with none of their "things" connected to the Internet.

Figure 1: Key Business Drivers for IoT Development

The IoT growth is driven by business needs as part of enterprise digital transformation (Fig. 1). According to Machina Research,5 the total number of IoT connections will grow from six billion in 2015 to 27 billion by 2025. It means a compound annual growth rate (CAGR) of 16%. In terms of market growth, the Berg Insight report5 predicts an increase of the global third party IoT platform market from €610m in 2015 to €3.05bn in 2021.

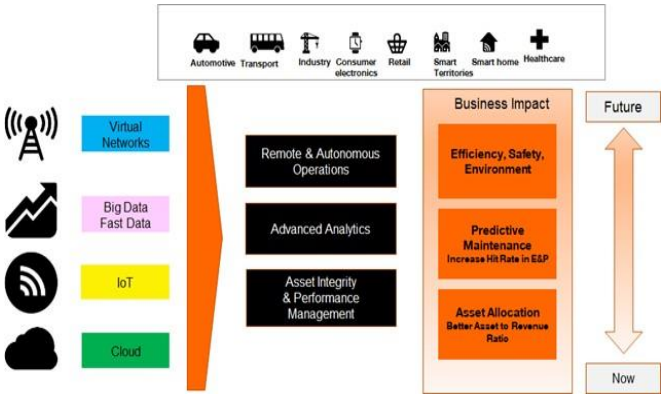

Figure 2 : IoT Connecting Technologies and Disparate Industries

II. LITERATURE REVIEW

The authors in [2] stated that there are various challenges, such as jamming and spoofing attacks and other unauthorized access, which have compromised the integrity of the user's data. There are potential solutions that can help the individual to implement various security measures that can help to secure their IoT devices. According to [1], various privacy threats have emerged in the present time, and they can penetrate IoT Technologies and their integrated network. It is not easy to manage the security of IoT devices in businesses and organizations. The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Traffic interceptors and analyzers help identify and investigate various cyber threats.

There are various studies as well as services that have been conducted on the current trends in IoT security [3]. Multiple services have presented some of the challenges or attack vectors to various IoT devices and their guards. Various simulation tools, modelers, and the availability of numerous platforms that can confirm this security protocol can also help in producing the protocol related to novel IoT security. It is fair to say that there has been rapid progress in terms of research related to IoT security and various simulation tools as well as modelers have supported this research. If the IoT devices failed, then the issues will be severe.

The authors in [4] believe that, despite the enormous benefits the users are getting from the Internet of Things, there are challenges that come along with it that need to be looked at. Cybersecurity and privacy risks are the primary concerns that have been cited. These two are posing a massive predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet, requiring novel security solutions. On the other hand, it is important to emphasize the standards and basic principles of the IoT Cyber Security Framework when it comes to implementing the IoT security system. According to [3], one of the most important measures to consider is the termination of a contract consisting of different devices with different communication protocols. The difference in protocols hinder separate service contracts from implementation and are fundamental elements that must be present in the cybersecurity structure of every Internet of Things. He demonstrated that to ensure the reliability of the IoT framework in the cybersecurity arena, some small steps need to be taken to help mitigate the challenges of IoT cybersecurity. In addition, the authors in [5] showed that scalability is also an essential measure

of the success of the cybersecurity Internet of Things framework. Analysts said the IoT environment needs to be scalable enough to handle a billion Internet-related and cybersecurity challenges. In addition, the magazine showed that the IoT cybersecurity environment should also support testability, such as integration testing, component testing, system testing, and compliance testing, effectively reducing challenges and risks. In the same context, the authors in [6] described some of the current IoT cybersecurity solutions.

Some basic security measures are implemented by the supplier, and state that it is not profitable for the supplier to produce high-quality solutions. In the case of cybersecurity of the Internet of Things, companies are unlikely to develop the right solution.

Moreover, the authors in [3] describe the currently embedded mobile and cyber-physical systems as ubiquitous, from industrial control systems, modern vehicles to critical infrastructure. Current trends and initiatives, such as Industry 4.0 and the Internet of Things (IoT), promise innovative business models and new user experiences through strong connectivity and the effective use of new generations of embedded devices. These systems generate, process, and exchange large amounts of relevant data. Security and confidential beliefs that make cyber attacks an attractive target for the Internet of Things system cause physical harm and disrupt people's lives. Cybersecurity and privacy are important because they can pose a threat. The complexity of these systems and the potential impact of cyber attacks pose new threats to related industrial IoT systems. Possible solutions to security and privacy challenges are general security frameworks for industrial IoT systems. Current IoT systems have not improved enough to secure the desired functions.

Therefore, there has been extreme significance in the study and research of various security issues in IoT. One of the main objectives in terms of IoT security is to provide privacy, confidentiality, and to ensure that every user can get better protection, infrastructures, and a guarantee to the availability of various services offered by the ecosystem of IoT. Therefore, the research in various IoT security is gaining necessary momentum with the help of different simulation tools as well as multiple computational platforms [2].

III. SECURITY ISSUES IN IOT NETWORKS

The same basic security objective of Confidentiality, Integrity and Availability that should be available for all interactions using computers and networks are needed to check the security of IoT. However, the IoT has many restrictions and limitations in terms of the components and devices, computational and power resources, and even the different and pervasive nature of IoT that introduce further studies to be addressed with respect to organising security. This section consists of two parts: the common security characteristics that the IoT must have, and the security problems peculiar to each layer of the IoT.

Security Features of IoT

The security challenges of IoT can be broadly divided into two classes; Technological and Security objection [5]. The technological challenges come due to the different and pervasive nature of IoT devices, while the security provocation is related to the ethics and usefulness that should be implemented to attain a secure network. Security should be included in IoT throughout the growth and running lifecycle of all IoT devices and hubs [4].Given below are the security principles that should be followed to achieve a secure interaction framework for the people, software, processes, and things in an IoT.

Confidentiality- It is important to ensure that data is secure and only available to approved users.
Integrity. The IoT is based on interchanging data and information between many various types of devices, which is why it is important to confirm accuracy of the data; that data is being comes from the right sender as well as to make sure that the data is not modified with during the process of transmitting due to intended or unintended interference.

Availability. The vision of IoT is to join as many smart devices as possible. The users of the IoT should have all the data visible whenever they need it. However data is not the only modules that is used in the IoT; devices and services must also be approachable and accessible when needed in a timely fashion in order to achieve the predictions of IoT.

Authentication-Each object in the IoT must be clever to clearly identify and authenticate other objects. However, this process can be testing because of the nature of the IoT; many entities are mixed up (devices, people, services, service providers and processing units). In addition, sometimes objects may need to communicate with other objects for the first time (objects they do not know). Because of all this, a methods to mutually authenticate entities in every communication in the IoT is required.

Lightweight Solutions-All of the security intentions considered earlier is not peculiar to IoT, although it may add special characteristics and constraints to each of them. However, in general confidentiality, integrity, availability and authentication are treated as basic intention in every computer or network security.

Figure 3: IoT Security principles

Heterogeneity- The IoT connects different entities with contrasting potential, complexity, and vendors. The devices even have desperate dates and discharge versions, use desperate technical interfaces and bitrates, and are designed for an altogether different functions. Therefore obligations must be outlined to work in a variety of devices as well as in distinctive situations. The IoT aims at connecting device to device, human to device, and human to human, thus it implements connection between different things and networks. One more challenge that must be considered in IoT is that the environment is always changing (dynamics), at one time a device might be linked to a completely distinctive set of devices than in another time. And to ensure security optimal cryptography system is needed with an adequate key management and security protocols.

Policies-There must be policies and standards to ensure that data will be managed, protected, and transmitted in an efficient way, but more importantly a mechanism to accomplish such plan is needed to assure that every entity is implementing the standards. Service Level Agreements (SLO) must be clearly identified in every service involved. The enforcement of such guidelines will recommend trust by human users in the IoT model which will hereafter result in its growth and scalability.

Key Management Systems- In IoT, the devices and IoT sensors need to interchange some encryption materials to achieve confidentiality of the data. For this intention, there needs to be a lightweight key management system for all structures that can

enable trust between different things, and can deliver keys by consuming devices minimum capacity.

IoT connectivity requirements are very diverse (Fig. 4) and, as a result, various types of communication technologies are used (Fig. 4, Table 1).

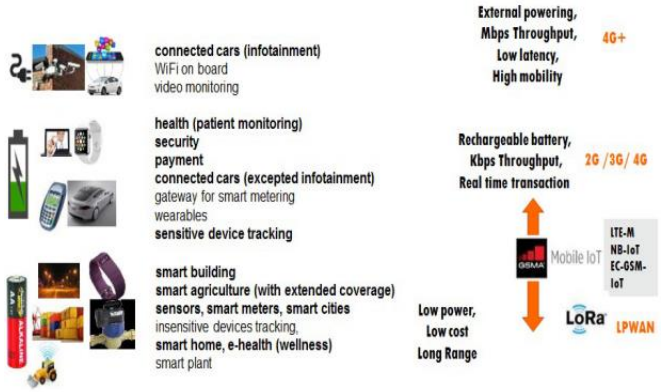

Figure 4: IoT Connectivity Requirements

Various communication technologies have been deployed by enterprises to implement IoT solutions (Table 1):

Table 1: IoT Communication Technologies

	LR-WPAN	LoRaWAN	BLE	RFID
Standard	IEEE 802.15.4	LoRaWAN R.1.1	IEEE 802.15.1	ISO/IEC 18000
Frequency band	868/915/2450 MHz	868/900 MHz	2.402 – 2.481 GHz	125 or 134 KHz for Low- Frequency RFID;13.56 MHz for High-Frequency RFID systems, 860 ~ 960 MHz for Ultra High Frequency RFID
Transmission range	10-20 m	Several km (2- 5 km in urban areas and 15 km in suburban areas))	10-100 m	Up to 100 m (active tag)
Data rate	40-250 Kbps	0.3-50 Kbps	The theoretical over-the air data rate is 1 Mbps (the LE 1M PHY Layer transfer rate). The practical application throughput depends on many factors and is reported as 10-20 Kbps.[22,23]	6.7 - 848 Kbps (HF Passive)
Energy consumption	Low	Very Low	Very Low	Low
Cost	Low	High	Low	Low
Article section	6.2.1	6.3.1	6.2.3	6.2.5

As seen from Table 1, two main categories of networks used in the IoT are short-range and long-range low power networks. We will consider security aspects of each of these types.

IV. FUTURE OF THE INTERNET OF THINGS

Currently, objects and systems are empowered with network connectivity and have the computing power to communicate with similar connected devices and machines.

Expanding the network capabilities to all possible physical locations will make our life more efficient and help us save time and money. However, connecting to the Internet also means to communicate with potential cyber threats. Internet-enabled products become a target for cybercriminals. The expansion of the IoT market increases the number of potential risks, which can affect productivity and the safety of the devices and hence our privacy. Reports highlight the frequencies of data breaches have increased drastically since 2015; 60% in the USA only. Another survey conducted in Japan, Canada, the UK, Australia, the USA, and France discovered that 63% of the IoT consumers think these devices are creepy due to improper security. Research findings also highlighted that 90% of consumers are not confident regarding IoT cyber security.

Current research explored various innovative techniques to mitigate cyber attacks and increase privacy solutions. Some of the solutions identified through the research are listed below;

Deploying encryption techniques: enforcing strong and updated encryption techniques can increase cybersecurity. The encryption protocol implemented in both the cloud and device environments. Thus, hackers could not understand the unreadable protected data formats and misuse it.

Constant research regarding emerging threats: the security risks are assessed regularly. Organizations and device manufacturers developed various teams for security research. Such teams analyze the impact

of IoT threats and develop accurate control measures through continuous testing and evaluation.

Increase the updates frequency: the device manufacturers should develop small patches rather than substantial updates. Such a strategy can reduce the complexity of patch installation. Besides, frequent updates will help the users to avert cyber threats resources from diverse sources.

Deploy robust device monitoring tools: most of the recent research proposed to implement robust device monitoring techniques so those suspicious activities can be tracked and controlled easily. Many IT organizations introduced professional device monitoring tools to detect threats. Such tools are quite useful for risk assessment, which assists the organizations in developing sophisticated control mechanisms.

Develop documented user guidelines to increase security awareness: most of the data breaches and IoT attacks happen due to a lack of user awareness. Usually, IoT security measures and guidelines are not mentioned while users purchase these devices. If device manufacturers specify the potential IoT threats clearly, users can avoid these issues. Organizations can also design effective training programs to enhance security consciousness. Such programs guide users to develop strong passwords to update them regularly. Besides, users are instructed to update security patches regularly. The users also taught and requested to avoid spam emails, third-party applications, or sources, which can compromise IoT security.

Everybody is looking forward to the fate of IoT and what it is holding for the future. There will be more than 30 billion IoT devices by 2025. Earlier on, people were aware of the IoT project, but they discarded the idea by looking at how the idea looked complex and challenging to implement. However, after the development of technology, it is now dawning on people that this was not impossible as the level of IoT development is scaling new heights day by day. In 2020 and beyond, for instance, intelligent thermostats and smart lighting are a few examples of how IoT is being used not only in the preservation of energy but also in the reduction of the bills and this contributes to the great reason why many people are choosing IoT devices.

A lot of cities will become smart. In the development of cities, there will be completely new horizons with the use of IoT. There will be better management of traffic; the roads will be free from congestion, the cities will benefit from reduced pollution, security will be of high standards all this by the implementation of IoT to a large scale.

Healthcare services are becoming much costlier, with the number of chronic diseases on the rise. We are approaching a time where primary healthcare would be complicated to get for many individuals, especially as people are becoming more prone to diseases. However, even though the technology is not capable of stopping the population from aging, it can help in making healthcare easier on the pocket in terms of accessibility. For instance, by moving routine medical checks from the hospital to the patient's home, this will be a massive relief to the patients. Real-time monitoring using devices connected to the Internet of Things is one of the ways that will help save the lives of many patients. On-time alerts are very critical in the instances of life-threatening circumstances, as many medical IoT devices will continue to be connected to gather vital data for real-time tracking. The quality of life of the patients will be significantly improved.

V. CONCLUSION

Internet of Things security is an active research topic in research industry and academia. It needs further attention and study to explore different

security problems in IoT. This paper investigate major security problems in each layer of IoT four layers architecture i.e. perceptual layer, network Layer, support Layer and application layer. The security issues in support layer has not been explored so far in the context of IoT.

VI. REFERENCES

[1]. International Telecommunication Union – Telecommunication Sector, Series Y: Global Information Infrastructure, Internet Protocol Aspects and next Generation Networks - Frameworks and functional architecture models - Overview of the Internet of things, Y.2060", June 2012.

[2]. Vermesan and P. Friess, Eds. ERC Cluster SRIA 2014 – Internet of Things – From Research and Innovation to Market Deployment. River Publishers Series in Communication, 2014.

[3]. The Internet of Things Reference Model. Cisco, June 2014.

[4]. Laeeq and J. A. Shamsi. A Study of Security Issues, Vulnerabilities, and Challenges in the Internet of Things. In Securing Cyber-Physical Systems. Taylor and Francis. Oct 2015.

[5]. N. Jeyanthi. Internet of Things (IoT) as Interconnection of Threats (IoT). In: Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. Fei Hu (Ed). CRC Press, 2016.

[6]. Sugandhi Maheshwaram, "A Comprehensive Review on the Implementation of Big Data Solutions", International Journal of Information Technology and Management Vol. XI, Issue No. XVII, November-2016

[7]. Sugandhi Maheshwaram, "An Overview of Open Research Issues in Big Data Analytics", Journal of Advances in Science and Technology, Vol. 14, Issue No. 2, September-2017

[8]. Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.

[9]. Sudheer Kumar Shriramoju, "Capabilities and Impact of SharePoint On Business", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2, Issue 6, November-December-2017.

[10]. Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016

[11]. Sudheer Kumar Shriramoju, "An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014

[12]. Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level Security", Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012

[13]. Sudheer Kumar Shriramoju,, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013

[14]. Sudheer Kumar Shriramoju, "SECURITY ISSUES, THREATS AND CORE CONCEPTS OF CLOUD COMPUTING", Airo International Research Journal, Volume IX, Feb 2017.

[15]. Malyadri. K, "An Overview towards the Different Types of Security Attacks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2014

[16]. Malyadri. K, "Security Threats, Security Vulnerabilities and Advance Network Security Policies", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 9, September 2013

[17]. Malyadri. K, "Need for Key Management in Cloud and Comparison of Various Encryption Algorithm", International Journal of Scientific

Research in Computer Science, Engineering and Information Technology , volume 1, issue 1, July-August 2016

[18]. Malyadri. K,"A STUDY ON EXPERIENCES ANDLIMITATIONS OF MOBILE COMMUNICATION", Alochana Chakra Journal, Volume VI, Issue VIII, August 2017

Cite this Article

Yeshwanth Valaboju , "IOT Communication Technologies and Future of Internet of Things", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 6, pp. 1437-1444, November-December 2017.

Journal URL : http://ijsrcseit.com/CSEIT1833695