International Journal of Recent Engineering Science (IJRES)
ISSN: 2349 – 7157 / doi: 10.1445/23497157/IJRES-V7I3P101
Volume 7 Issue 3, 1-6, May-Jun 2020

Security Issues Faced By Internet of Things: A Survey

Preetha S[1], Sagar J[2], Krishna Pooja P[3]
[1,2,3] *Department of ISE, B.M.S. College Of Engineering, VTU, Bengaluru, India*

Abstract

IoT Security (IoT) is the field of technology relating to the safety of IoT networks and embedded machines. IoT requires the application of internet access to an integrated computer network, mechanical and digital equipment, artefacts, animals, and persons. The IoT is a multi-machine network that allows data and information to be exchanged, including vehicles and internet-connected home appliances. Data may also be shared with people and items or objects. There may be some sort of mixture. IoT refers to the digital devices found in Cloud, circuitry, applications, cameras, actuators, and access to the network. This includes other different programs, from infrastructure, healthcare, intelligent buildings, construction. The internet-based, IP-based networking and development protocols allow an exchange of smart topics' information on insecure networks. This paper discusses IoT protection in three forms: i) security of communication; ii) security of computer; and iii) security of knowledge. The purpose of the paper is to include a review of IoT's research and to provide advice and accessible questions for potential studies.

Keywords - *Internet of Things (IoT), Wireless Network, Protection, Privacy, Communication Technologies*

I. INTRODUCTION

Internet of Things (IoT) involves networking real artefacts – installed in a network that collects and exchanges information on computers, devices, cameras, and actuators. IoT combines all the various forms of the network, from tiny or big computers, household equipment, body apps, and cloud networking, like the state networks, Telephone, omnipresent networks, and vehicles. Internet of Things (IoT) is a complex, wireless, or wired, auto-configuration network, which focuses on usual and interoperable networking with titles, physical and virtual artefacts, and digital character can intelligently and utilize. The IoT comprises many forms of networks from local, online, regional, and car from the sensor to the new cloud technology. Developments in IoT can choose specific communication methodologies and architectures with various available technologies. Specific aims and technologies can be used to build IoT systems. RFID, Ethernet, ZigBee, or Wi-Fi can be chosen for short-range communication. Some choose ZigBee for industrial automation systems, and WiMAX or Cellular technologies may be the alternative for long-range communication. Traditional protection mechanisms cannot be used explicitly because the smart devices in terms of computing, memory, and bandwidth are hungry for space. This paper's reference to numerous polls that we have done in this report and evaluating other existing IoT security-related initiatives, outlines the current vulnerability to IoT.

We have addressed using computer securing, program interface securing and protected data sharing, and IoT will still follow simple safety specifications. We have addressed using computer securing, program interface securing and protected data sharing, and IoT will still follow simple safety specifications. Section II outlines the wireless networking technologies. Section III discusses how we can achieve IoT security. The remainder of the paper is organized into four different parts. In that respect, we are still concerned about particular future research—the strengths and pitfalls of IoT. In Section V we analyze the current technology and the literature review. In Section IV, we are debating. In Section VI, the paper ends and provides a reference to potential work for students.

II. WIRELESS COMMUNICATION TECHNOLOGIES

The backbone of such IoT networks is wireless networking technologies that allow connectivity between different equipment and numerous supporting applications.

NFC: Near Field Communication is a network that allows consumers to exchange data and expertise between NFCs permitted devices at high frequencies and short-range (13,56MHz). NFC will become a big networking technology in the future, irrespective of the above explanation. NFC provides fast network connectivity and sharing of knowledge, without any handshaking. NFC can be changed to provide a consumer function and much-improved usability of the device. This also offers multi-level data security, which is really one of IoT's focal points. The room is one of the significant disadvantages NFC has.

RFID: Radio frequency identification is a device that allows for remote analysis of the details put on a microchip without the usage of physical communication equipment. Different frequency ranges include RF, a medium frequency, high frequency (125 kHz), a too high frequency (433 MHz), and a microwave (2.45 GHz). RF contains various frequencies. If the power transferred is usually small, a specific band frequency may not require a license.

Bluetooth: IEEE 802.15.1 complies with Bluetooth. This is a low-power, cheap wireless networking system that can share data between mobile phones from 8 to 10 meters. Bluetooth explains network-to-personal area (PAN) Synchronization. Data sizes vary from 1 to 24 Mb / s for specific Bluetooth applications. This platform's ultra-low-power, the inexpensive version is Bluetooth Low-Energy (BLE or Bluetooth Smart). BLE has previously been released in 2010 with Bluetooth platform v4.0. Communication Protocol enables computers to connect with various devices and exchange network details. The following is a summary in Table1 on just several networking techniques.

Wireless HART: Wireless HART is a sensor system explicitly based on a highway HART protocol. The specific specifications for Wireless HART were set and built for process field computer networks as a multi-provider, interoperable wireless device. Regularly used for authorization inside the 2.4GHz ISM spectrum, the protocol utilizes IEEE 802.15.4 radios.

6LowPAN: In order for IEEE 802.15.4 networks to submit and receive IPv6 packets. IPv4 and IPv6 are delivery mechanisms such as telephones for central, national, and internet networks. 802.15.4 IEEE also offers communication capability sensing for Wireless Domain Systems. Moreover, the fundamental structure of the two networks is distinct. The IEEE 802.15.4 nodes will either operate securely or improperly. Two safety modes are specified in the specification to achieve separate security aims: access control list mode (ACLM) and protected mode.

WiMAX: IEEE 802.16 is the wireless networking instruction kit. The WiMAX specifications include a bandwidth rate between 1.5Mb/s and 1GB/s. (Worldwide Microwave Interoperability Connectivity).

Mobile network: There are several types of cell networking systems, including 2G (including GSM and CDMA), 3G (including UMTS and CDMA2000), and 4 G (including LTE). In other terms, IoT systems may communicate across cellular networks. The operating performance of these requirements is about 9,6 kb/s (2G) and 100 Mb/s (4G). In other terms, IoT systems may communicate across cellular networks. For such amounts, the service limit ranges from 9.6Kb/s (2G) to 100Mb/s (4G) and is accessible on the 3GPP website. Figure 1 depicts the 6LoWPAN Adaptation Layer.

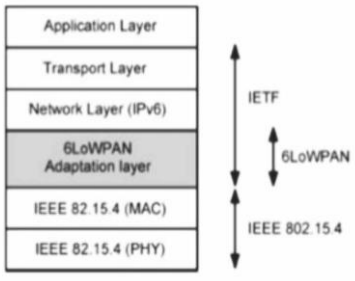

Fig1. 6LoWPAN Adaptation Layer

III. HOW TO SECURE INTERNET OF THINGS

Although more conventional networks are not fully protected, so it is still a machine issue on how to protect them properly. A device that is still based on a traditional architecture framework that also needs specific criteria is much more prone to security threats. With the IoT business rise, the data and IP of the organization need more than ever to be guarded. All developers must obey the following resources in order to ensure that all IoT apps are secure

Authentication: The next problem for IoT is authenticating the authentication of IoT customers. With the new modern protocol, authentication and self-configuring are more complicated compared to the conventional approach. E.g., utilizing two-factor authentication, Google double-stage verification, particularly with the help of a mobile device that remains with you, allows monitoring the application a little simpler. The characteristics that make your mobile an efficient surveillance tool stay the same and allow our watches, bracelets, and thermostats to insight into and express our personality.

Confidentiality of personal data: Third parties will easily intercept IoT posts with the help of modern technology. For instance, other people access their home application from the restaurant's public Wi-Fi to view some live video. Accessing similar content from home to third parties on the same network will be fast. So confidentiality is quite essential, and correspondence from intermediate entities needs to be protected. Confidentiality of end to end message (E2E) in IoT is necessary. Besides, data gathered on IoT devices should be guaranteed against unauthorized parties, such as contact information and personal details.

Data integrity: The majority of IoT's privacy-based function, which is also a core component of IoT protection, is impressive. Integrity is far greater than accessibility, as confidentiality may contribute to embarrassment but integrity, significantly if the damaged medical system or vehicle mechanism, quickly costs someone's life. The Keyless Signature Infrastructure (KSI) and PKI are used as an external data feature.

Access Control: Access controls in the conventional system are only applied to a closed network where the network is open to all users. In IoT, an open and closed structure where an unknown party plays a significant role should be considered.

Communication Security: Providing security services mentioned in the section above would require secure contact in the IoT. Through using uniform protection protocols, we will have the protection of contact at various levels.

IEEE 802.15.4 Layer: Bridge Level Encryption Correspondence. 802.15.4 The new cutting-edge IoT protection approach is the reliability of connector layers.

The security of the link-layer avoids per-hop contact in which nodes must be trusted on the communications path. A single pre-shared key is used for encrypting all messages. Usually the protection of the connection layer is restricted where an intruder has breached a device and access to a specific key, but it is incredibly scalable and operates on different layers with several protocols.

Networks of 6LoWPAN: 'IPv6' was used to facilitate sensor node connectivity. IPv6 should also be used in IoT as it also allows it easy to set up, manage, customize, and monitor the network. The IETF has set up a 6LoWPAN working party to develop IEEE 802.15.4 LoWPAN IPv6 support, distinguished by a more integrative layer of links with network speeds. Three distinct styles of LoWPAN architecture models were established.

- Ad-hoc LoWPAN
- LoWPAN provided with a one edged router
- LoWPAN provided with multi-sided routers

The Protection 6lowPAN Architecture aims to enhance the protection relations between a newly authenticated device and an individual who wants to link the domain without allowing external intermediaries to obtain any visibility into the key information shared. The first machine to encounter is acquainted with its neighbours' titles. After that, the machine is authenticated.

Network Layer: IP Security: it requires network Access Safety (IPsec) as a network layer-supported IoT that is effectively implemented on the internet. IPsec offers security, confidentiality, and integrity through end-to-end encryption. IPsec provides IP payload protection and integrity using the Encapsulated Protection Payload (ESP) protocol and TCP header and payload integrity with the Authentication Header (AH) protocol. IPv6 is now needed in IPsec, which guarantees default support for all IPv6 apps.

Abstraction Layer: Each device is connected to wire internet and wireless home networking, which is a hot topic with the growth of home care. A wide variety of devices, regions, environments, and topologies may be handled utilizing various networking schemes. As for each application of the network, other network issues ought to be addressed.

IEEE 1905.1's design is modular and scalable to accommodate potential domestic networking growth. The 1905.1 Abstraction Layer (AL) includes protocols that can relay network or system-borne packets. The layer of 1905.1 requires a little alteration in the underlying home network infrastructure. The behaviour or functionality of the current home networking technologies does not then change.

Data Security: Connectivity- Securing is an essential part of IoT, but most app developers fail to encrypt data from all the IoT apps. Most IoT systems are lightweight and lack adequate protection due to the restricted size and shielding capacity from the security risks associated with hardware components. There are several solutions available, but due to the different networking systems, even one approach cannot be sufficient to secure anything.

IV. ADVANTAGES AND DISADVANTAGES OF IoT

Over these many years, the Internet-of-things has revolutionized to an expansive degree. Some of the main advantages of IoT

- ***Cost reduction:*** It helps the automated systems to communicate effectively with each other, thereby reducing and saving resources and energy; thus, it supports people in their daily lives. IoT essentially facilitates our processes by allowing data to be shared and transferred between electronic devices and then transformed into our required form.

- *Information:* It is true you can make better choices with more details. If it is general decisions like knowing what to buy in a grocery store or getting enough supplies and accessories in your business, information is a great power, and more information is always healthy.
- *Communication:* IoT correspondence enables synchronization from machine to machine (M2 M) (synchronization between devices). The physical processes will, therefore, stay connected; thus, it is possible to obtain total continuity with greater output and lower inefficiencies.
- *Automation and control:* There is a great deal of automation and tracking in the processes leading to the controlling and remote contact of specific items via cellular networks. All computers can interact without human intervention and therefore lead to prompt performance.
- *Increased Efficiency:* Improved production Increased output plays a key role in the success of a company. IoT gives guidance to the workers just in time.

Some of the main disadvantages of IoT:

- *Over Dependence on Technology:* Currently, it is observed that the younger generation is a technology freak, and for any little thing, they depend on technology and its tools. With the aid of IoT, this attachment in everyday tasks can become even more so. No program is safe from fault, and every technological framework involves several hitches. Entirely depending on IoT devices will cause difficulty in an IoT network struggling to operate or crashing.
- *Losing Privacy Protection:* When different technology and devices are involved, surveillance is carried out by more than one organization, specifically questions security and privacy issues. The collection and storing of data often is a big problem for businesses, and at the same moment, they both operate. In the case of having just one

business, this can contribute to the problem of hegemony.

- *Lesser job opportunities:* With IoT, day-to-day operations are streamlined, and there would inevitably be less human capital needs and few trained workers, which will trigger job challenges in the community.
- *Complexity:* There is the probability of fault in all complex structures. Failures in the Internet-of-Things situation may be skyrocket.

V. LITERATURE SURVEY

Over the last years, the future Internet of Things health services has been able to relieve the burdens of the health care sector. This work then incorporates state-of-the-art studies on the capabilities, limitations, and general health of a wearable IoT medical device for each model area. IoT healthcare faces challenges such as stability, privacy, and guidelines for the potential directions of science[1]. The architecture of sophisticated physical, cyber systems (CPSs) is focused primarily on wireless sensors and Internet-of-Things (IoT) connection actuators. This paper discusses wireless connectivity principles from the standpoint of IoT and the networking criteria of CPS. We then review the most relevant wireless security principles based on certain definitions and concentrate on the main safety concerns. Real examples and recent attacks especially point to the disparity between the communications securities in CPS and IoT communications protocols and their actual faults and vulnerabilities [2].

In [3] particular in non-traditional technologies (e.g., oil and gas industries), the commercial Internet of Things (IoT) is emerging. However, several IoT and property monitoring issues exist, including the usage of coding and other data storage and maintenance strategies. They analyzed the new development in the 21 papers published in this particular version. We conclude with a set of potential research plans on the current problem. The IoT is a classic emergent idea, developed as an interconnected network of billions of lightweight, state-of-the-art devices programmed to achieve real-life insufficiency. In the past decade, the concentration of IoT science has evolved as a core mechanism for the continuous incorporation of human behaviour into IT. This paper summarizes existing IOT work that has illuminated emerging technologies, such as Fog-based computation, WLAN, Data Mining, and background awareness [4].

Significant cyber hazard widening is likely due to the inherent vulnerabilities in IoT products, with scarce capital and heterogeneous technology, along with a lack of explicit IoT norms. This essay attempts to organize the panorama of the defence of information technology that offers taxonomical study in the context of the three central layers of the IoT model system: 1) understanding, 2) mobility, and 3) stages of operation. In the study, we should concentrate on the most important questions to lead potential directions for science and future research works [5]. A considerable amount of data is continuously generated by the Industrial Internet of Things (IoT). It is unwise to locally store all raw data on IoT platforms, as the finishing systems have strict resource and storage capacities.

Furthermore, computers are untrustworthy and susceptible to several threats because network operations may be implemented remotely. This post addresses the current problems of data management, safe data storage, significant data recovery, and advanced IoT data collection. Then we build a scalable and economic system to solve the problems faced by Fog and cloud infrastructure convergence. The data obtained is analyzed and deposited on the edge server and cloud storage, depending on time latency specifications [6].

IoT is the next phase in contact. The IoT allows the production, processing, and transparently sharing of data through physical artefacts. For this nature's environment to be applied even more successfully, high protection, safety, authentication, and recovery from attacks are needed. To build end-to-end, stable IoT ecosystems, significant improvements are essential in the design of the IoT applications [7]. The Internet of Things (IoT) has achieved immense attention in the world today; the IoT community expands and reveals how the future looks in the days ahead.

Nevertheless, protection is still a challenge to IoT systems, as they are built for low power and limited sized installations. The IoT field is not impeccable. Protection algorithms are not harsh, but many of them are not appropriate for IoT systems because the usability of them can only depend on the more developed products (meaning generally improved output, storage). The main concern was to analyze the performance and evaluate the processing time of different protection algorithms [8].

In order to encourage computing resources to be implemented at the network level. In order to enhance customer interface and stability of the networks in the event of a malfunction, Fog and advanced computing are suggested to be combined with Internet-of-Things (IoT). Fog / Edge computing for IoT implementations should provide fast reactions and higher operating efficiency, with centralized network benefit and near to end-users. This study discusses IoT in-depth in the field of system architecture, enabling fog/edge measurement as well as IoT deployment, infrastructure, safety, and data security concerns, and includes a detailed overview of this objective [9]. The Internet of Things (IoT) is a new technology that has revolted over the global human network, intelligent machines, electronic tools, knowledge, and data. This paper analyses the security of IoT information thoroughly. Heterogeneous autonomous systems and ICT technologies are the critical paradigms for the safety and functionality of these goods. The review includes cybersecurity studies, such as existing IoT cybersecurity studies, IoT cybersecurity, and taxonomy

design, fundamental countermeasures and techniques, and main applications [10].

Internet of Things (IoT) applications for customers are becoming increasingly popular. We discuss in this article the design and functions of existing common smart home platforms. Then we address the issues of protection, privacy, and the state of the art initiatives suggested by these platforms. In order to obtain unauthorized entry and perform an over-privileged activity that violates the safety of the consumers, we have carried out a detailed study of many different antiques on the voicing. To measure the proposed program's efficiency, we introduce a specific testbed on Samsung's SmartThings platform [11]. IoT is a technology that ensures all-inclusive Internet connectivity and transforms artefacts into mobile devices every day. The IoT model shapes the relationship between people and their physical artefacts. There are benefits not just for mobile applications but also for the manufacturing climate. We saw the IoT definition in recent years with beautifully designed solutions finding their way into the industry. Within this article, we address its processing and business values. We give a thorough overview of state-of-the-art testing efforts and potential recommendations to address industrial IoT problems[12-15]. Table1 reflects a summary of IoT research.

VI. CONCLUSIONS

The IoT has now been a huge part of modern life without many of us even knowing it. If technology continues to evolve and expand, IoT can be used for several of our essential experiences. It is up to us to determine how much we like technology to govern our everyday lives. Nevertheless, if implemented correctly, it can eventually conform to our desires to help humanity as a whole. Many organizations are focusing on safety protocols to provide a genuinely accessible network where people will receive secured contact, secured device access, protective data transfer to shopping. The production of IoT includes a popular norm for manufacturers, vendors, and businesses and is regarded as a priority.

IoT defence has to be built into the app to address security issues. If safe data is compromised, it may lead, in particular in medicine, to severe consequences. Protective measures planned for the system must be taken into account in development. However, the reliability of the system can be modified with time. Constructing network protection alone cannot provide a full IoT defence, but this is indeed the potential. Through its lifespan, IoT reliability will be debated. As we spoke about in the previous chapter, the Web was designed mainly for networking and not connecting millions of computers. In the future, the amount of IoT devices will increase, and it all depends on how network security can be handled at any point. Hence, recognition of specific requirements and protocols for receiving security in the IoT is of utmost importance.

REFERENCES

[1] Stephanie Baker, Wei Xiang, Senior Member, IEEE, and Ian Atkinson., Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities.(2017).

[2] Andreas Burg, Member IEEE, Anupam Chattopadhyay, Senior Member IEEE, And Kwok-yan Lam., Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things.(2018).

[3] Kim-Kwang Raymond Choo, Senior Member, IEEE, Stefanos Gritzalis, and Jong Hyuk Park., Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities.(2018).

[4] IKRAM UD DIN1 et al. Senior Member, IEEE., The Internet of Things: A Review of Enabled Technologies and Future Challenges. (2018).

[5] Mario Frustaci, Pasquale Pace, Member, IEEE, Gianluca Aloi, Member, IEEE, and Giancarlo Fortino, Senior Member, IEEE., Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. (2017).

[6] Jun-Song Fu, Yun Liu, Fellow, IET, Han-Chieh Chao, Senior Member, IEEE, Bharat K. Bhargava, Fellow, IEEE, Zhen-Jiang Zhang, Member, IEEE., Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing (2018).

[7] VIKAS HASSIJA et al., A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures.(2019).

[8] Nuzhat Khan, Nazmus Sakib, Ismot Jerin, Shaela Quader, and Amitabha Chakrabarty., Performance Analysis of Security Algorithms for IoT devices, Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh, IEEE.(2017).

[9] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao University., A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Conference. (2017).

[10] Yang Lu, Member, IEEE, Li Da Xu, Fellow, IEEE., Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics.(2018).

[11] Yan Meng, Wei Zhang, Haojin Zhu, and Xuemin (Sherman) Shen, IEEE., Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures.(2018).

[12] Emiliano Sisinni, Member, IEEE, Abusayeed Saifullah, Member, IEEE, Song Han, Member, IEEE Ulf Jennehag, Member, IEEE and Mikael Gidlund, Senior Member, IEEE., Industrial Internet of Things: Challenges, Opportunities, and Directions. (2018).

[13] Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu, Member, IEEE., The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, Internet of Things Journal.(2018).

[14] Mauro Contia, Ali Dehghantanhab, Katrin Frankec, Steve Watson., Internet of Things security and forensics: Challenges and opportunities.(2018).

[15] Prof. Manisha G. Gedam1, Mr Waibhav K. Deogade2 Assist. Prof., G. H. Raisoni., The Severe Effect of IoT Characteristics on Security and Privacy: Threats, Existing Solutions, and Challenges, Institute of Information Technology, IEEEE Journal.(2017).

[16] I.Lakshmi., A Study On The Internet Of Things And Cyber Security With Intruders And Attacks, International Journal of P2P Network Trends and Technology 9(3) (2019) 4-13.

[17] Jisha C.T, Mamatha Balachandra, Derroll David., Survey on Internet of Things (IoT): Security issues and countermeasures, International Journal of Engineering Trends and Technology (IJETT). 46(5) (2017) 271-275.

Table 1: Summary of IoT research

Authors (Year)	Methodology used	Findings	Cost Effectiveness	Power Consumption	Range	Application	Data rate
Stephanie Baker et al. (2017)	Bluetooth and ZigBee	Bluetooth is better and cost effective than ZigBee	Bluetooth is cheaper as it is already installed on mobile phones	Very Low	<10cm	Easy set up for health care sector	400kbps
Andreas Burg et al. (2018)	UHF RFID	Narrow band spectrum gives better results	Very Cheap	Very Low	<100m	Identification and communication with ultra-low costs	40 - 640kbps
Raymond Choo et al. (2018)	Cryptographic techniques	Can be used with other technologies for better performance	Varies Slightly with increase in number of devices and devices	Very Low	–	Security of Data at Industrial IoT	Remains same
Ikram Ud Din et al. (2018)	NB-IoT	Flexibility in Deployment	Cheaper when used GSM for communication	Low	15km	Worldwide Coverage	250kbps
Mario Frustaci et al. (2017)	ZigBee	Data Leakage and Malicious Injections are avoided	Moderate	Low	10 - 300m	Sensor networks and Industrial automation	250kbps
Jun-Song Fu et al. (2018)	Cloud computing and fog computing	Using kNN Algorithms to enhance privacy-preserving	Moderate	Moderate	–	Industrial IoT handling large amounts of data	Remains same
Hassija et al. (2019)	Block Chain	Data encryption using the hash key	Moderate	Moderate	–	Smart IoT devices	Remains same
Nuzhat Khan et al. (2017)	Crypto ++ with RFID	getRSA is the most efficient algorithm	Moderate	Moderate	<100m	Under constrained environment, this is used	40 - 640kbps
Jie Lin et al. (2017)	Z-Wave	Simple in implementation	Cheaper than ZigBee	Low	<1km	supports 232 with greater reliability	Up to 300kbps
Yang Lu et al. (2018)	Wireless networks	ensure confidentiality in IoT	Low	Moderate	200m	Industrial sensing networks	250kbps
Yan Meng et al. (2018)	6LowPAN	IPv6 packets to be sent and received	Slightly high	Slightly high	800m	Sensor network building	250kbps
Emiliano Sisinni et al. (2018)	Wireless HART	Easy setup, can be used anywhere	Low	Slightly high	<50m	Internet, Multimedia	700kbps
Wei Zhou et al. (2018)	Wi-Max	constrained and interdependence IoT features	High	High	50km	Broadband, internet connectivity	10 - 100mbps
Mauro Conti et al. (2018)	SigFox	Narrow Band Modulation	High	Very High	30km	Regional coverage	100mbps
G. H. Raisoni et al. (2017)	LoRa	Seamless and integrated service	Very High	Very High	Upto 60km	Worldwide coverage with high security	Upto 600 kbps