A SURVEY OF INTERNET OF THINGS

Anshita Dhoot,
Department of Radio Engineering & Computer Technology, Moscow Institute of Physics & Technology, Moscow, Russia
anshita.dhoot.23@gmail.com

A.N. Nazarov,
International Telecommunication Union, ITU, Moscow, Russia
a.nazarov06@bk.ru

DOI: 10.36724/2664-066X-2020-6-2-25-32

ABSTRACT

The growing era of technology through the internet, Internet of Things (i.e. IoT) has a powerful and strong industrial system that provides an opportunity to grow and applications to use ubiquitously. Its applications use sensor, wireless, mobile and RFID technology devices. In recent years IoT applications are enhancing to being deployed as well as developed. The IoT promises to have a great future era of the Internet uses that involves machine-to-machine communication. It helps to enable the sensor network as well as technologies, even IoT got involved in our day-to-day routine such that it supports to control and to monitor a human being's mundane by providing mobile access, remotely. Undoubtedly, remote access is the incredible feature of the IoT which has been given to this world. The main objective of IoT is to provide remotely accessible at low-cost that too by often visits through electronic devices. This paper presents the maximum possibilities of challenges, applications, security issues and techniques of IoT.

KEYWORDS: *Internet of Things, IoT devices, applications, Technologies*

Information about authors

Anshita Dhoot, *Department of Radio Engineering & Computer Technology, Moscow Institute of Physics & Technology, Moscow, Russia*
A.N. Nazarov, *Prof., International Telecommunication Union, ITU, expertMoscow, Russia*
ResearcherID: G-3154-2013. Scopus Author ID: 7201780424

I. Introduction

In the era of growing the leverages of smart electronic devices with a high speed of IoT. It has gained a wide range of popularity with acceptance as the standard for the resources which have network constrain. Those embedded devices and network things that have sensors which are interconnected through the networks either private or public [1-3]. The IoT devices can be organized remotely so that one could perform the desired functionality. In terms to share the information by using these devices via a network that employs some standard communication protocols, which has been set for security purpose. As figure 1 shows the connectivity held in between the IoT devices, it doesn't matter wherever the devices are, this requires the wireless network, appliances, devices that support network connectivity.

The upcoming years of IoT will change the real-world objects into smart virtual objects. The smart devices which are used to get connected vary from wearable devices to the huge machines, where each device is having sensor chips to connect. Few of IoT devices are Lenovo smart shoes have sensor chips to support the fitness data to track and to analyze, even electrical appliances such as refrigerators, washing machines, microwaves, etc. can be accessed and controlled easily from a remote location, and the most renowned devices for IoT is the surveillance cameras that can be controlled remotely, no matter wherever a person is in this world [4, 5]. IoT has taken over the community requirements too, apart from the field of the electronic devices for personal use.

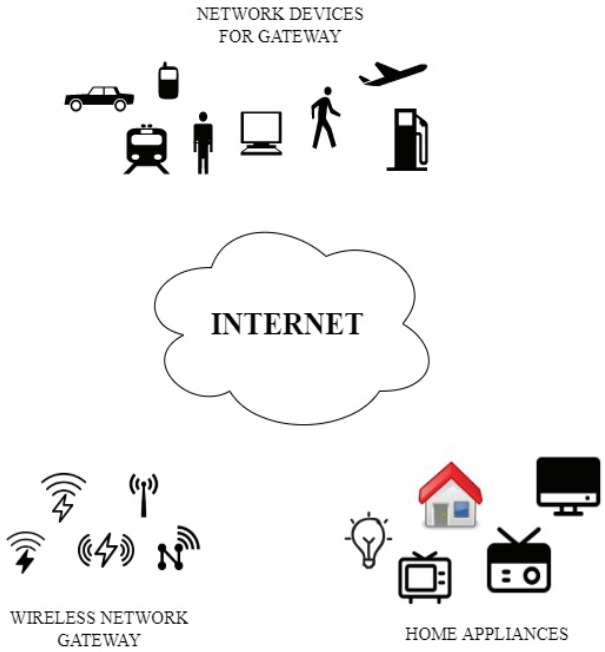

Figure 1. IoT Overview Model

The plethora of smart devices give diversity to use its functionality such as to monitor a surgery, to detect the weather predictability of its condition, automobiles connectivity, to track or to identify an animal, etc. there are uncountable areas where IoT serves the whole community whichever needs it. The data which has been collected through those electronic devices that process in the real-time that improves the efficacy to the complete system. The futuristic IoT significance is evident because of its application which has been used in mundane life. In the case of growing field of IoT that evolves the rapid growth of the hardware techniques to improve the bandwidth through the incorporating cognitive radio which is based on the network that addresses under-utilization of the frequency spectrum [6,7].

Since the paradigm of IoT represents the interconnected networks collection as well as the heterogeneous devices. So, it inherits the issues of conventional security that is related to computer networks. Moreover, the resources constrain challenges towards IoT security of its sensors and devices that have limited memory and power.

If we go back to see the previous years of IoT makes a tremendous effort to cope with its security issues, that approaches to have end-to-end IoT security. A recent survey [8], categorizes the issues arises in the security of IoT during the application, data, communication as well as architecture. The IoT threats are there for hardware, software, applications as well as network components. There are security issues to analyse has been discussed by Granjal el.al [9]. The analysis of security has been presented and discussed by the work done by the researcher has been shown in the paper [10-15]. This targets an evaluation for Intrusion Detection Systems (IDS), comparatively. If it comes to provide the analysis of the issues in security of IoT the fog computing has been presented by the scientific work in the papers [16-18]. The contributions towards the IoT that provides security, access control, privacy, and confidentiality that also includes the security of the middleware layer [19]. These authors discuss the issues in IoT related to the privacy, security of data, trust management, the security of the network, authentication, as well as IDS.

Scientific researchers have searched the preservation mechanisms for privacy in IoT. Many researchers describe the security of computing multi-party security to enforce preventing IoT users' privacy. The credit mechanism to check and to attribute base on access control has been described as solutions to effect preservation of privacy. The possible threats and countermeasures for IoT based on cloud, many research works are there to identity and node compromising, location privacy, to add or to remove the layer, as well as key management for IoT threats while using cloud [20-22]. The architecture of the IoT compliance needs to implement privacy, security and trust. The trust model expects to provide data confidentiality as well as data integrity while end-to-end communication makes possible by the mechanism for authentication. Furthermore, to evade improper data usage, the model for privacy needs to define access mechanisms and policies to decrypt and encrypt data [23].

The rest paper has been organized as follows. In Section 2, the security in IoT will be delineated. Section 3 includes the architecture of IoT. After all of the preservatives towards the IoT security and its hindrances, technologies of IoT will be discussed in section 4. In Section 5, challenges in IoT details are there, whereas Section 6 includes the possible applications in the field f IoT, before concluding the paper in Section 7.

II. Security Issues in IoT

2.1 What is IoT?

The IoT itself a wide range, and it is hard to define IoT in few words, the unique definition that is available universally acceptable by the world of IoT community users. "The IoT is an open, as well as a comprehensive network of the smart and intelligent objects, are capable to auto-organize data and resources, sharing information, to react and act in the situation as well as to be able to change inside the environment." The IoT continues to be the most hyped and latest concept in the world of IT [25].

The IoT has already attracted many lives and attention by its vision for a network of physical objects for global infrastructure that enables anytime, connectivity at any place from one to many things at a single time [26]. IoT has been introduced as a global network that allows the human-to-human, things-to-things, and human-to-things communications. It could be anything that connects as well as communicate smartly or intelligently better than ever before [27].

2.2 Requirements for IoT setup

IoT is the huge world in itself. It is not the work of 2-3 machinery as a part of the setup. It requires the need to secure hardware as well as software. This requires a large setup with a lot of embedded real-time connectivity use to build a proper IoT. To implement the IoT successfully, it requires the following:

- Dynamic Resource Demand
- The need for Real-Time
- The demand for exponential growth
- Applications availability
- Protection of Data
- Privacy of Users
- Applications to consume efficient power
- To execute the applications for nearby end-users

Apart from above-mentioned prerequisites, IoT needs to access in an open as well as an interoperable cloud system. This required the basic three components that are needed for seamless IoT and its computing.

- Hardware: In IoT hardware required the composition of the sensors, CCTV, embedded devices to communicate, actuators, IP cameras, etc. which are needed to connect a hardware device to help in communication.
- Middleware: In IoT, this is required to store the data and also supports the computing tools to analyse data with the analytical power of Cloud and Big Data.
- Presentation: This is the broadcasting part of IoT, that helps to visualize the data and an interpretation tool that can be used to design several other applications.

2.3 Security for IoT

In terms to deploy the security, [28] several parameters and mechanisms are required to be estimated which is mentioned below:

- *Privacy, Integrity and Confidentiality of Data (PIC)*

IoT is a huge platform to travel the data to communicate which passes through the multi-hops exist in the network; a proper mechanism to encrypt is needed to ensure the data confidentiality. It happens because of the assorted network, device and services to store the data on any device is prone to violate privacy rules of compromising nodes that exist in the IoT network. The IoT device is vulnerable to the attack that causes an intruder to impact the integrity of data by modification of data storage for malicious purposes.

- *Availability of Services*

The attacks on the devices in IoT hinder the service to provide by the conventional Denial-of-Services (DoS) attacks. Several schemes include the jamming intruders, sinkhole attacks or replay attacks that exploit the components of IoT at different layers to wane the QoS to provide IoT users.

- *Accounting, Authorization, and Authentication (3A).*

IoT communication security requires the authentication in between the two parties to give them the legal access for their privilege services, for this, an authenticated device is mandatory. The mechanism of authentication's diversity for the existence of IoT is lying majorly for the heterogeneous diversity for its fundamental architecture and its environment that supports devices of IoT. These ambiences pose a challenge to define its standard protocol globally to authenticate in IoT. Correspondingly, the mechanisms to authorize for ensuring the system access or to provide authorized user, it needs a proper authorizing implementation and authenticating implementation results in a reliable environment to ensure an environment to secure communication. Accounting of the resource usage, with its auditing as well as reporting, gives a trustworthy mechanism to secure the network management.

- *Efficiency for Energy*

The devices in IoT are typically resource-constrained as well as are characterized by less storage and low power. The IoT architecture results in an enhancement to consuming energy by network flooding and IoT resources exhausting by forged and redundant service request.

III. IoT Architecture

At the end of 2020, 25 billion things are expecting to be connected [29] which is in a large number, so the existing Internet Architecture with the TCP/IP protocols which have been adopted in 1980 [30] that cannot able to handle a huge network as large as the IoT that cause a need for the latest open-architecture that address different security as well as QoS issues and it supports the existing applications of the network by using the open protocols [31]. Without an appropriate privacy assurance, as IoT is not likely in terms of adopting by many IoT users [32]. Hence, the fortification of IoT users' privacy and data are major IoT key challenges [33].

According to the further IoT development, a number of the multilayer architectures for security have been proposed. As per the paperwork [34], describes the three-key level of IoT architecture, whereas [35] mentioned the four-key IoT architecture level of its security, and [36] described the five-layer architecture by using the superlative features of Internet and Telecommunication Management architecture based on the TCP/IP as well as TMN models, respectively. Correspondingly, six multilayered architecture has been proposed which is based on the hierarchical structure of the network [37]. As shown in figure 2, about the six-layer architecture of IoT which have been described below in details:

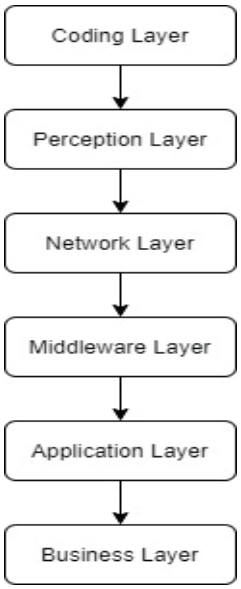

Figure 2. IoT Architecture Layers

- Coding Layer: This is the foundation layer of IoT that provides identification to the interest objects. In this layer, each object is allocated a unique ID that makes it much easy to discriminate the objects [37].
- Perception Layer: In this layer, a physical meaning is provided to each object. It constrains the sensors of data in distinct forms such as RFID tags, IR sensors and other networks of sensors [38] that could able to sense the humidity, location, temperature, speed, etc. of the objects. This layer collects the important information of each object from its sensor devices which is linked with them as well as converts the existed/received information into the digital signals so that they can pass for the further action on the Network Layer.
- Network Layer: This layer having the aim to receive the important information that too in the form of the digital signals from its second layer i.e. Perception Layer as well as transmit it to its processing system exists in its fourth layer i.e. Middleware Layer by the transmission medium such as Bluetooth, WiMax, WiFi, Zigbee, 3G, GSM, etc. with its protocol such as IPv6, IPv4, DDS, MQTT, etc. [39].
- Middleware Layer: In this layer, the information is received from its sensor devices [40]. It contains technologies such as ubiquitous computing that assures the direct access to its database to collect the entire important information in it. By using the Intelligent Processing Equipment (IPE), the processed information, as well as a fully automatic action, has been taken which is based on its information for its processed results.
- Application Layer: In this layer, IoT applications for all type of industries that are based on its processed data due to the promotion of its application to develop the IoT, so this application layer is very important in the large scale to develop the IoT network [36]. Those applications which are related to the IoT for smart transportation, smart homes, smart planet, etc.
- Business layer: In this layer, helps to manage the IoT applications as well as services which are responsible for all the IoT related research. It creates various business model to affect business strategies [41].

IV. Technologies of IoT

Initially, IoT was inspired by the community of RFID to discover information possibility to tag the object for browsing an address of internet or database entry of internet, so that it correspondingly for an RFID or its near field communication technologies [42]. In the paperwork [43], technologies related to IoT such as RFID, nanotechnology, intelligence embedded technology, and the sensor technology have been introduced. Other technologies such as RFID, 2D barcode, and NFC allow identifying the physical objects to refer over the internet. IoT integrated the RFID with sensor technologies, so that hardware devices can get connected with the internet resources, ubiquitously. The trending IT industry waves, since the computing field application, global roaming technology and communication network technology has been applied. Additionally, it includes the sophisticated technologies of communication network and computer, so that it could support the IoT technologies, for instance, remote communication technology, information technology, remote information transmission technology, controlling technology, sea measures intelligence analyzes, etc. [44-46].

- *RFID*

Radio Frequency Identification (RFID) transmits an object's identity or a person's identity through the radio wave, wirelessly, in the form of given serial number. The major RFID components are antenna, reader, access controller, server, reader and software [47]. It is more secured, reliable, accurate, efficient and inexpensive. It has extensive wireless applications range for instance patient monitoring, tracing, military apps, distribution, etc [48].

- *EPC*

Electronic Product Code i.e. EPC, a 64 bit and 98-bit code on an RFID tag that is electronically recorded and envisioned to create an enhancement in the system of EPC barcode. EPC global organization is responsible for its standardization of EPC technology that has created the EPC global network, to share the RFID information. It has main four components i.e. EPC Discovery Service, Object Naming Service, EPC Security Services, and EPC Information Services.

- *Barcode*

This is just a distinct way to encode numbers as well as letters to use the bar combination and to space the changing width. [49], Barcode is optical on the machine to read labels which are attached to its items to record the related item information. In recent times, the system of QR code becomes renowned outside the industry of automotive because of its huge capacity to store and to read faster as compared to the standard. Majorly, three kinds of the barcode are there i.e. Numeric, 2 Dimensional and Alpha Numeric. This is designed to read by the machine. Generally, it is readable by the laser scanners. It can be readable by using cameras.

- *Wi-Fi*

Wireless Fidelity i.e. Wi-Fi, is a technology for networking to allow the computers as well as its other devices for communicating over the signal wirelessly. The father of Wi-Fi is Vic Hayes. [50], the predecessor to Wi-Fi has been invented by NCR Corporation in the year of 1991, in Nieuwege, Netherland. The very first wireless products have been brought on the market with its speed 1

Mbps to 2 Mbps, under the name of WaveLAN. Millions of WLAN connectivity has been delivering Wi-Fi at homes, offices, even at the public or private locations such as café, metros, restaurants, railway stations, airports, etc. There are a lot of technologies that contain the kind of WLAN product to support IEEE 802.11 with dual-band, 802.11b, 802.11a, 802.11n and 802.11g.

- *IP*

IP stands for Internet Protocol. This is the crucial network protocol which is used on the internet. It has been developed in the years of 1970s. The principal communication protocol is IP, exists in the Internet protocol suite to relay datagrams over the boundaries of the existing network [42]. It has five classes that range in the IPv4 i.e. Class A, Class B, Class C, Class D, and Class E, whereas only the Class A, B and C are majorly used classes. The real protocol gives the 4.3 billion addresses of IPv4, although, IPv6 will be ominously argument the availability to the addresses up to 85000 Trillion. IPv6 is majorly used in this 21st century that supports addresses approximately 2^{128}.

- *ZigBee*

This is one of the protocols which have been developed to enhance the WSN's features. ZigBee Technology has been formed by the ZigBee Alliance in the year of 2001. The important ZigBee's characteristics which have low data rate, moderately short transmission range, scalability, low cost, flexible protocol design, reliability [51]. It is the wireless network protocol that has low power, based on the IEEE 802.15.4. ZigBee ranges around the hundred meters as well as 250 kbps bandwidth. The topologies of ZigBee work as a cluster tree, mesh, and star that is broadly used in digital agriculture, home automation, medical monitoring, power systems and industrial controls.

- *Bluetooth*

This is the technology that is short-range radio technology and inexpensive wireless technology. It eliminates the proprietary need of cabling in between the devices, for instance, notebook PCs, PDAs, handheld PCs, printers and cameras within its effective range i.e. 10 to 100 meters. Generally, to communicate via Bluetooth at less than 1 Mbps, it uses the IEE 802.15.1 standardized specification. Firstly, in the year 1993, Ericsson Mobile Communication Company initiated the project which is named as "Bluetooth", is the creation of PAN i.e. personal area network. Bluetooth device set shares a mutual channel to communicate which is known as Piconet. This Piconet can share data within 2 to 8 devices at a period, and this data could be a sound, video, text and picture. There are more than a thousand companies that comprise by Bluetooth Special Interest Group with Cisco, Intel, Ericsson, Motorola, Toshiba, Aruba, and HP.

- *Actuators*

It converts the energy into the motion. This means the actuator drives motion into the mechanical system. It takes electric current, hydraulic fluid and some different power source. It can create the rotary motion, oscillatory motion and linear motion. Typically, cover short distances up to 30 feet that can communicate less than 1 Mbps. It is used in the applications of industrial and manufacturing. Mainly, it has three kinds i.e. electrical, pneumatic and hydraulic, whereas electric actuators used commonly, hydraulic actuators and pneumatic actuators system allows increasing the torque and forcing from the smaller motor.

- *WSN*

Wireless Sensor Networks consisting the autonomous devices by using sensors to cooperate environmental conditions as well as physical conditions, for instance, sound, temperature, pressure, pollutants, vibration, at distinct locations. WSN is the most important element in the paradigm of IoT [52]. IoT based WSN has received incredible attention in several areas such as home security, military, accurate agriculture monitoring, healthcare, habitat monitoring, manufacturing, flood detection, forest fire, so on.

- *NFC*

NFC stands for Near Field Communication, is a set of wireless technology that is for short-range i.e. 13.56 MHz, which is approximately equal to the distance of 4 cm. This technology makes the life more convenient and easier for its users around the world to make it easy for exchanging the digital content, connect electronic devices and transactions, such that they could connect with a touch of electronic devices. It allows the wireless networks instinctual initialization of NFC complementary to the Bluetooth. 802.11 With its capacity up to 10 cm to support its long-range distance. It works in the untidy environment that doesn't need the line of sight simple as well as easy for the connection method. It has been first invented by the Sony and Philips companies. In this, 424 kbps is the data exchange rate, whereas the consumption of power during the time of reading data in the NFC which is under 15 ma.

- *AI*

Artificial Intelligence i.e. AI refers environment of electronic that is responsive as well as sensitive in the people's presence. In an ambient smart world, electronic devices work in the concert to support the people for carrying out their mundane life activities in a natural way to use the Information & Intelligence which is in its connected network devices, hideously. This system has characteristics such as context awareness, embedded, adaptive, anticipatory, and personalized.

- *Cloud Computing*

This is the only technology that analyzes as well as store the data. Intelligent computing technology has an ample amount of server are congregated on one platform of cloud that allows resource sharing to be accessed at any place or time. It is the most valuable part of IoT, apart from converging sensors, it also processes on enhanced analyzes, and power of the important information which is received by the sensors as well as provide the good space capacity to store data. The potential of cloud computing contains the zillionths of sensors that give a massive advantage, as well as help IoT to be dependent over cloud computing.

- *Optical Technologies*

The increasing fast development in the field technologies that includes optical technologies, such as Cisco's BiDi and Li-Fi, it could be an important breakthrough in IoT development.

- *Nano Technologies*

The smallest and enhanced version of the interconnected things, it can reduce the system consumption by making it enable for device development with the nanometer scale, to be used as an actuator and sensor as a

normal device. This Nano device has been made up of nano-components that result in networking to define a new paradigm that uses the Nano-things on Internet.

- *Network Technologies*

In the IoT success, these technologies have played an important role. This is the huge network that provides a connection between the objects. It provides us with the effective, huge and fast network that covers a huge number of the devices which is potential in the network. This modern era fully dependency over ubiquitous computing needs super powerful, super-efficient, as well as super-fast growing generation of the wireless system. Likewise, short-range communication between the network, technologies like Wi-Fi, Bluetooth, Infrared, etc. are famous to use.

- *MEMS*

This micro electro mechanical system (MEMS) is a combination of the mechanical and electrical components that work together for providing the numerous applications to include actuating and sensing, that uses it commercially in various areas in the form of accelerometers as well as transducers. The combination of MEMS and Nanotechnologies provides a cost-effective solution to improvise the IoT system communication. The other benefit is to reduce the size of actuators and sensors to integrate the computing devices ubiquitously, as well as the frequency higher range.

V. IoT PRIVACY CHALLENGES

With the help of using IoT, everything seems easy as it makes a person and an object addressable and locatable to make human life easier comparatively than earlier, however the lack in the confidence about the privacy and security to the data of the users. The ubiquitous adoption of the IoT that have a sturdy secure infrastructure, even though it includes some concerns related to its privacy as below:

- *Breaching Sensor Nodes Security*

The sensor vulnerability by the attacks includes the bidirectional sensor network. The other data transmission, data acquisition is possible too. The attacks including tampering, flooding, jamming, Sybil, and other attacks make breaching of the sensor nodes, even after providing the best possible security system.

- *Abusing Cloud Computing*

The huge network of the cloud computing that converge servers by allowing the resource sharing in between them, such kind of sharing resources faces a lot of threats in there security such as phishing, man-in-the-middle, etc. There are important steps that have been taken to ensure the security of IoT. Cloud Security Alliance i.e. CSA has been introduced a few possible threats such as Data Loss, Malicious Insider, Hijacking Accounts, Monstrous use of computer sharing, and others.

- *RFID Illicit Access*

The tags in RFID help to access the authenticated user as it contains the details about the users. The exposure of any credential information or data of the user by any unauthorized user can create severe damage to the user data. Few real-life RFID threats include side channel, RFID virus, SpeedPass Hack, or other attacks that could harm the data.

- *Limitation of Resources*

The resource-guarded IoT architecture is the major hindrance to define the security mechanism robustly. Contrastingly, those paradigms which are conventionally limited by the cryptographic algorithms to work under those constraints that provide multicasting as well as broadcasting which is needed to exchange its certificates or the key. This storage and energy are needed to cope with in the situation to provide an accomplished implementation for communicating IoT protocols with complete security. Entailing the protocols are redesigning to be ample energy-efficient and light-weighted, despite needing the complex structure of computations to improve the techniques for energy harvesting.

- *Security Protocols Interoperability*

IoT mechanisms for its global security for standardizing it and its protocol so that it could be implemented at the different layers which are required to be interoperated by using the conversion mechanism. It becomes effectively by using the security standards combination lying at each layer, within the global mechanism.

- *Range of Heterogeneous Devices*

This gives the vast range to vary from small sensor devices that have low power to the high-end servers, which is needed to be implemented in the security framework of multi-layer security. It makes itself to adapt in the environment with the existing resources, to make the decisions related to the selection of the IoT layers security mechanisms, before the process to provide the services to the end-users. Dynamically adapting the security framework of the IoT architecture's required intelligence, such that resources standardization in the IoT architectures can be deployed.

- *Failure Single Points*

There are numerous architectures, networks, and protocols exist in the paradigm of IoT, heterogeneously. Due to this reason, it becomes more deployable to each existing point. Mechanisms of IoT and its standards have been introduced to reduce the redundancy to keep in the view for trading-off in-between the reliability and the cost of its complete infrastructure.

- *Trust Managements & Updates*

This is the most open issue for the future work into research that provides trust management and the scalable management, and to update the existing software into zillions of IoT devices. The major problem with its relatable data is to make it reliable and secure for the owner of the IoT device by the government. Data Privacy, as well as Supply Chain, is the open research area for the researcher as it has violation in the wide range. Block technology is enabling for the solution to secure IoT, even though, this itself impose the research challenges to be handled through its efficiency, key collision, regulations, scalability as well as arbitration.

- *The Vulnerability of Firmware/Hardware*

The low power, as well as low cost devices, is ubiquitously becoming trendy. In this, IoT architecture becoming more exposed to the vulnerabilities related to its hardware, not related to its physical malfunctioned. Even, the algorithm implementation for its security lying in its hardware, packet as well as routing to process its mechanisms which requires verification before IoT get de-

ployed. There is a different standard to verify the protocol, so that no intruder can crack the existing system.

- *Vulnerable BlockChain*

The security of IoT is robust and approaching for the system of block-chain which is highly vulnerable. The mechanism is depending on the power of miner hashing that can be compromised in a few manners. Sometimes, the attacker hosts the block-chain to make the private key for limiting the random exploitation. Its efficient mechanism is needed to define the assurance of the transaction privacy, that avoid attacks in a race that gives result the double spending, during the time of transaction.

VI. IoT APPLICATIONS

Mostly, mundane leveraging applications we normally visualize them user-friendly and easy to communicate with each other. It helps to use a wide range of information sharing for pioneering applications. Several existing emerging applications provide autonomously capable to enhance the quality of living standards. Majorly, real-time applications are becoming popular such as a self-driving car with the traffic evaluating by real-time, conditions of road as well as the weather or some other crucial information that is being exchanged by those applications of IoT. Few of IoT applications are mentioned below in this section.

- Smart Environment: It helps to predict the natural calamities which are going to happen in the coming future such as earthquakes, flood, etc. It is possible because of the emerging innovative IoT applications that help to monitor environmental pollution.
- Smart Traffic System: It makes enables to detect the congestion in transportation, that provides the feature such as reporting accidents, detection of being theft, traffic jam, climate-changing situation, etc. It provides the smart city idea to manage a traffic system according to the existing situation by predicting it through the IoT applications.
- Smart Hospitals: IoT applications are quite renowned in the flexible hospital environment by using the RFID tag to evaluate patient's blood pressure, oxygen level, heart rate, temperature, etc. It helps a lot during the time of emergency while cardiac attack.
- Smart Home: For monitoring the household utilities such as water supply, energy consumption and meters. These IoT applications help to save the utilities by detecting in advance so that it could save the wastage of water, electricity or other household utilities. For instance, the garden gets water as per their need, or alarm will buzz while water leaks, and so on.
- Smart Retailing: RFID with IoT provides benefit to the supply chain or the retailers. In this, equipped RFID products can be tracked in the existing stock, so that it could get detected during shoplifting. It helps to track overstock, sales chart as well as effective strategy graph.
- Smart Agriculture: The IoT application helps in monitoring the light, soil nutrition, humidity, etc. so that it helps to improve the GreenHouse experiencing by the automatic adjustment of the temperature for maximizing the production. The precise level of water and fertilization to improve the quality of water as well as to save the fertilizers.

VII. CONCLUSION

Gradually, IoT is bringing incredibly technological changes in people mundane life. It turns into help for making a happier life which is comfortable, simple and easy to live due to the various applications and technologies of IoT. IoT is universally standardized with no standard definition. User-to-user application has been varying that needs to be interoperable. IoT is there to use for global governance with standard protocols for better future. This is vast in its usage by its applications into areas such as industrial, transportation, governance, implementation, habitat, education, mining, medical, etc. The global mechanism to secure the IoT layers is important due to its diverse IoT resources. This paper outlined future research areas for making IoT more efficient, scalable, and reliable for its security solutions.

References

1. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future Generation Computer Systems* 82 (2018), pp. 395-411.
2. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54.15 (2010), pp. 2787-2805.
3. Giusto, Daniel, et al., eds. *The internet of things: 20th Tyrrhenian workshop on digital communications*. Springer Science & Business Media, 2010.
4. Heater, B. "Lenovo shows off a pair of Intel-powered smart shoes, 2016." *URL https://techcrunch.com/2016/06/09/lenovo-smart-shoes*.
5. Rouse, Margaret, et al. "Drone (unmanned aerial vehicle, UAV)." *Internet of Things (IoT) news, blogs and analysis–IoTAgenda.com* (2016).
6. Khan, Athar Ali, Mubashir Husain Rehmani, and Abderrezak Rachedi. "Cognitive-radio-based internet of things: Applications, architectures, spectrum-related functionalities, and future research directions." *IEEE wireless communications* 24.3 (2017), pp. 17-25.
7. Akhtar, Fayaz, Mubashir Husain Rehmani, and Martin Reisslein. "White space: Definitional perspectives and their role in exploiting spectrum opportunities." *Telecommunications Policy* 40.4 (2016), pp. 319-331.
8. Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." *Journal of Network and Computer Applications* 88 (2017), pp. 10-28.
9. Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." *IEEE Communications Surveys & Tutorials* 17.3 (2015): 1294-1312.
10. Roman, Rodrigo, et al. "Key management systems for sensor networks in the context of the Internet of Things." *Computers & Electrical Engineering* 37.2 (2011), pp. 147-159.
11. Granjal, Jorge, et al. "Why is IPSec a viable option for wireless sensor networks." *2008 5th IEEE international conference on mobile ad hoc and sensor systems*. IEEE, 2008.
12. Cirani, Simone, Gianluigi Ferrari, and Luca Veltri. "Enforcing security mechanisms in the IP-based Internet of things: An algorithmic overview." *Algorithms* 6.2 (2013), pp. 197-226.
13. Alrajeh, Nabil Ali, and Jaime Lloret. "Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks." *International Journal of Distributed Sensor Networks* 9.10 (2013), pp. 351047.
14. Abduvaliyev, Abror, et al. "On the vital areas of intrusion detection systems in wireless sensor networks." *IEEE*

Communications Surveys & Tutorials 15.3 (2013), pp. 1223-1237.

15. Ning, Peng, and Dingbang Xu. "Learning attack strategies from intrusion alerts." *Proceedings of the 10th ACM conference on Computer and communications security*. 2003.

16. Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." *International conference on wireless algorithms, systems, and applications*. Springer, Cham, 2015.

17. Wang, Yifan, Tetsutaro Uehara, and Ryoichi Sasaki. "Fog computing: Issues and challenges in security and forensics." *2015 IEEE 39th Annual Computer Software and Applications Conference*. Vol. 3. IEEE, 2015.

18. Sicari, Sabrina, et al. "Security, privacy and trust in Internet of Things: The road ahead." *Computer networks* 76 (2015), pp. 146-164.

19. Roman, Rodrigo, Javier Lopez, and Masahiro Mambo. "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges." *Future Generation Computer Systems* 78 (2018), pp. 680-698.

20. Oleshchuk, Vladimir. "Internet of things and privacy-preserving technologies." *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*. IEEE, 2009.

21. Esposito, Christian, et al. "Security and privacy for cloud-based data management in the health network service chain: a microservice approach." *IEEE Communications Magazine* 55.9 (2017), pp. 102-108.

22. Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE, 2014.

23. De Loof, Jourik, et al. "Internet of Things–Architecture IoT-A Deliverable D1. 5–Final architectural reference model for the IoT v3.0."

24. OWASP, Top IoT Vulnerabilities. "URL https://www. owasp. org/index. PHP." (2016).

25. Madakam, Somayya, et al. "Internet of Things (IoT): A literature review. "*Journal of Computer and Communications* 3.05 (2015). P. 164.

26. Evangelos A, Kosmatos, Tselikas Nikolaos D, and Boucouvalas Anthony C. "Integrating RFIDs and smart objects into a UnifiedInternet of Things architecture." *Advances in Internet of Things* 2011 (2011).

27. Aggarwal, Renu, and Manik Lal Das. "RFID security in the context of" internet of things"." *Proceedings of the First International Conference on Security of Internet of Things*. 2012.

28. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future Generation Computer Systems* 82 (2018), pp. 395-411.

29. Sawicki, Artur. "The Internet of things." *World Scientific News* 48 (2016), pp. 89-96.

30. Hauben, Ronda. "From the ARPANET to the Internet. "*TCP Digest (UUCP)* (2001).

31. An, Jian, Xiao-Lin Gui, and Xin He. "Study on the architecture and key technologies for the internet of things." *Advances in Biomedical Engineering* 11 (2012). P. 329.

32. Li, Lan. "Study on the security architecture of the Internet of Things." *Proceedings of 2012 international conference on measurement, information and control*. Vol. 1. IEEE, 2012.

33. Srivastava, Lara, and T. Kelly. "The internet of things." *International Telecommunication Union, Tech. Rep* 7 (2005).

34. Chen, Wang. "An IBE-based security scheme on the internet of things." *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*. Vol. 3. IEEE, 2012.

35. Suo, Hui, et al. "Security in the internet of things: a review." *2012 international conference on computer science and electronics engineering*. Vol. 3. IEEE, 2012.

36. Wu, Miao, et al. "Research on the architecture of Internet of Things." *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. Vol. 5. IEEE, 2010.

37. Zhang, Minghui, Fuqun Sun, and Xu Cheng. "Architecture of internet of things and its key technology integration based-on RFID." *2012 Fifth International Symposium on Computational Intelligence and Design*. Vol. 1. IEEE, 2012.

38. Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." *Wireless personal communications* 58.1 (2011): 49-69.

39. Zhang, Ying. "Technology framework of the Internet of Things and its application." *2011 International Conference on Electrical and Control Engineering*. IEEE, 2011.

40. Shen, Guicheng, and Bingwu Liu. "The visions, technologies, applications and security issues of Internet of Things." *2011 International Conference on E-Business and E-Government (ICEE)*. IEEE, 2011.

41. Khan, Rafiullah, et al. "Future internet: the internet of things architecture, possible applications and key challenges." *2012 10th international conference on frontiers of information technology*. IEEE, 2012.

42. Madakam, Somayya, et al. "Internet of Things (IoT): A literature review." *Journal of Computer and Communications* 3.05 (2015). P. 164.

43. Want, Roy. "An introduction to RFID technology." *IEEE pervasive computing* 5.1 (2006), pp. 25-33.

44. Li, Baoan, and Jianjun Yu. "Research and application on the smart home based on component technologies and the Internet of Things." *Procedia Engineering* 15 (2011): 2087-2092.

45. Razzak, Faisal. "Spamming the Internet of Things: A Possibility and its probable Solution." *Procedia computer science* 10 (2012), pp. 658-665.

46. Shao, Wei, and Li Li. "Analysis of the development route of IoT in China." *Perking: China Science and Technology Information* 24 (2009), pp. 330-331.

47. Sun, Chunling. "Application of RFID technology for logistics on internet of things." *AASRI Procedia* 1 (2012), pp. 106-111.

48. Dawood, Moeinfar, Shamsi Hossein, and Nafar Fatemeh. "Design and implementation of a low-power active RFID for container tracking at 2.4 GHz frequency." *Advances in Internet of Things* 2012 (2012).

49. Grieco, A., E. Occhipinti, and D. Colombini. "Work postures and musculo-skeletal disorder in VDT operators." *Bollettino de Oculistica* suppl. 7 (1989): 99-111.

50. Pahlavan, Kaveh, et al. "Handoff in hybrid mobile data networks." *IEEE Personal Communications* 7.2 (2000), pp. 34-47.

51. Chen, Xian-Yi, and Zhi-Gang Jin. "Research on key technology and applications for internet of things."*Physics Procedia* 33 (2012), pp. 561-566.

52. Arampatzis, Th, John Lygeros, and Stamatis Manesis. "A survey of applications of wireless sensors and wireless sensor networks." *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005.* IEEE, 2005.