International Multidisciplinary Research Journal Reviews (IMRJR)

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

IoT: Exploring Intelligent Interfaces and Future Directions

Dr. Vijeyata Chauhan[1], Ms. Poonam Rani [2], Dr. Sanjay Kumar Singh[3]

Associate Professor Don Bosco Institute of Technology New Delhi -110025[1]

Assistant Professor, Don Bosco Institute of Technology Okhla Road New Delhi -110025[2]

Associate Professor, Don Bosco Institute of Technology Okhla Road New Delhi -110025[3]

Abstract: The Internet of Things (IoT) is transmuting the way we interact with the physical world, incorporating machine-to-machine communication to form a integrated network of smart devices. This paper is an inclusive study of the current state of IoT research, exploring its foundational concepts, architectural components, key applications, and emerging challenges. It investigates into the intelligent interfaces that enable whole communication and collaboration among devices using sensors, actuators, and processors. The core concepts of IoT, including its definition, characteristics, and the fundamental technologies that drive its development is discussed. Then the architectural components of IoT systems, outlining the various layers such as insight, network, and application layers, and the role of middleware in facilitating incorporation and interoperability are inspected.

The paper explores the varied applications of IoT across numerous spheres, including smart homes, healthcare, industrial automation, agriculture, and smart cities. For each application, specific use cases, benefits, and the impact of IoT on improving efficiency and enhancing handler experience are highlighted.
The paper also talks about the emerging challenges in IoT, such as security and privacy concerns, scalability issues, and the need for standardization. We analyze the current approaches to addressing these challenges and identify gaps that require further research.

Finally, we highlight latent future directions for IoT, considering the advancements in related technologies such as artificial intelligence, edge computing, and 5G. We discuss how these technologies can be united with IoT to create more smart, approachable, and self-directed systems, paving the way for new innovations and applications.
By providing a thorough overview of the current state of IoT and its future prospects, this paper aims to serve as a valuable resource for researchers, practitioners, and policymakers interested in the continued development and deployment of IoT technologies.

Key Words: IoT, Edge Computing, Field protocol, Cloud protocol

1.INTRODUCTION

The internet of things (IoT) refers to a network of interconnected physical devices entrenched with sensors, software, and other technologies that collect and exchange data. This interconnection allows for the creation of intellectual systems that can mechanize tasks, improve efficiency, and provide valuable visions. As the figure of connected devices remains to grow exponentially, the potential impact of IoT across various sectors is undisputable. The potential influence of the Internet of Things (IoT) across multiple sectors is evident, especially in health sector, transportation system, business, smart homes and education.
The present paper comprises of 8 Sections in 1st section definition and historical background with applications of IoT is discussed. In section 2 IoT technologies and its types are discussed, in section 3 applications of IoT are discussed. section 4 includes security and privacy issues, Section 5 talks about IoT platform and network, the key findings are marked in section 6, future scope are mentioned in section 7 and the paper ends with conclusion in section 8.

1.1 Definition and concept of IOT

Internet of Things (IoT) is capable of connecting one thing with another, where human-to-human connectivity is not essential. The objective of this technology is to perform various operations with ease to achieve many different goals. We can say that internet is not only a simple grid of computers, but rather a network of various devices i.e. at the same time IoT is a network of associated devices (a network of networks). It is possible that near in future billions of devices could be connected with internet [1].

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

1.2 Evolution and historical background.

As far as the evolution of interconnected electronic device is concerned the invention of telegraphs is the first ever such invention in which information/message is shared in coded language in 1960s[2], use of barcode and RFID for automated systems are the example of such coding language. Kelvin Ashton, (Britain) is the father of IoT who used the term first time while connecting food/supply chain of Procter & Gamble digitally. The device management in IoT is important so as to keep a track on connected devices and their proper functioning.

1.3 Key components and architecture.

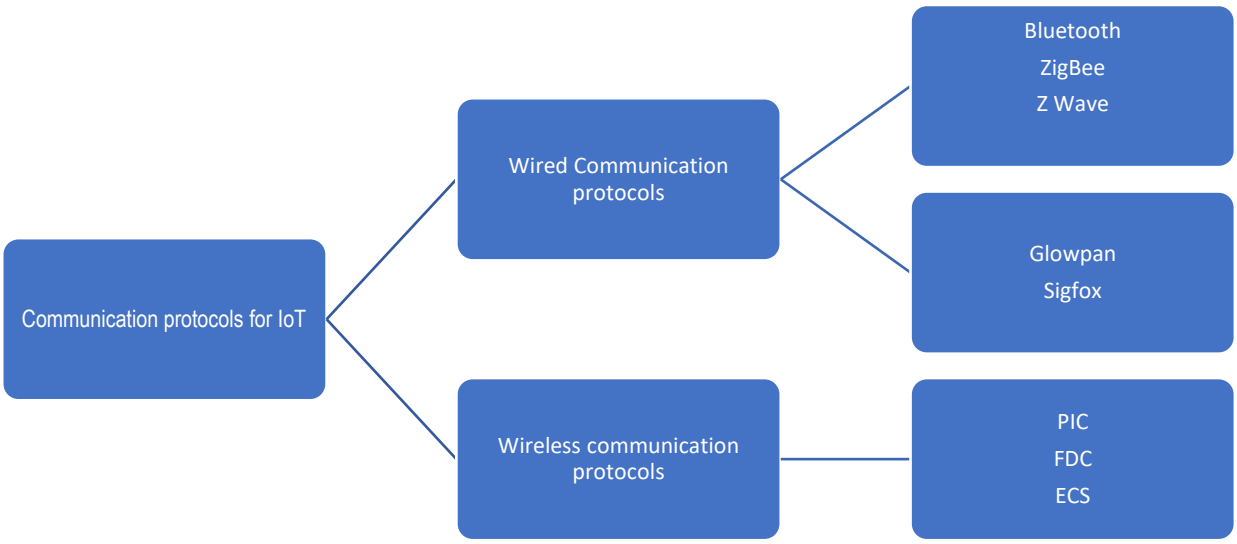
The key component of IoT architecture is mainly based on three layers : application layer, network layer and sensing layer. The data collection is done at bottom (sensing layer) from all the devices, middle layer (network layer) receives the data and these data are used at upper layer(application layer) for different purposes.

- **Perception Layer (sensing layer):** This layer comprises sensors that gather data from the physical environment. Sensors can be passive or active, measuring various parameters like temperature, pressure, or motion.
- **Network Layer :** This layer facilitates data transmission between devices and the cloud or local servers. This may involve numerous communication protocols like Wi-Fi, Bluetooth, or cellular networks.
- **Application Layer:** It processes the collected data, analyzes it, and generates meaningful insights or actions. It may involve cloud platforms, edge computing, and data analytics tools.

2. IOT TECHNOLOGIES

2.1 Wireless communication protocols

The communication protocols for IoT is classified as wireless communication protocols and wired communication protocols. The wireless communication protocol is a standard rulebook with reference to which various automated devices connect with each other wirelessly. The choice of wireless communication protocol depends on scope of IoT applications.



The major six types of wireless technologies are:

- **Cellular:** It has very high bandwidth and provide reliable broadband communication that supports everything and streamline the functioning. It works well in low power environments, especially with somewhat like Cat-M1. 5G technologies with ultra-low potential supports, the needs of thing like time -sensitive industrial automation, real-time delivery of therapeutic data and public safety surveillance.
- **Bluetooth and BLE (Bluetooth Low Energy) :** This is well known wireless service works in persona area network (WPAN), in short -range, BLE/Bluetooth are used in short -range communication and work effectively there , smart home devices and home security system are based on it.
- **WiFi –** This technology provide high speed data transfer and effective in smart home devices. It has more security risk as compared to other option of IoT.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

- **LPWAN:** Low power wide area network **(LPWAN)** provide long range communication facility using small, low-cost batteries. It supports large – scale networks but it can only send small blocks of data at a low rate. They can be effective in keeping standardization and ensuring the network's security , interoperability and reliability.
- **LoRaWAN:** LoRaWAN is similar to Bluetooth but it has long range data transfer facility at low power consumption. It is a pointtopoint wireless connection that doesn't have direct connection to internet while LPWAN is directly connected to
- cyberspace. It needs a gateway to forward data to cloud and for this LoRa cellular gateway is used. This technology is suitable for irrigation management, leak detection, logistics and transport management.
- **RFID -IoT:** Radio Frequency Identification (RFID) uses radio frequency signals to track and monitor objects for data transmission. It has unique identification number which can be tagged on sporting events, parking vehicles, loyalty cards and warehouse labels. RFID exchange information wirelessly but do not connect to the internet directly, To send data to cloud platform it requires cellular connectivity. It plays vital role in supply chain management.

2.2 Sensor Technologies and types.

Sensors in IoT collect the information from the surroundings and forward it to devices interconnected over internet. These sensors are helpful not only in security concerns, but in efficient use of energy and increases business opportunities for many industrial and corporate sectors. The various types of sensors are:
Temperature Sensors, Pressure Sensors, Accelerometer Sensors, Gyroscope Sensors, Biomedical Sensors, Motion Detection Sensors, Smoke Sensors, Proximity Sensors, Optical Sensors, Air Quality Sensors, Chemical Sensors, Flow Sensors, Level Sensors, IR Sensors.

2.3 Cloud computing and edge computing.

The processing of data is done using cloud computing and edge computing. Different applications of IoT are generating massive amount of data. To analyze and process this data is quite tedious, cloud computing, edge computing and fog computing are playing major role in processing these data.
Cloud computing is internet-based infrastructure that is used to access the data for storage and computing.[3] In early years data were stored by organization in their PCs and servers thus making the handling of such large server and physical devices difficult. On cloud computing large amount of data can be shifted from local to remote machines in cyber space. The services provided by Cloud computing are Infrastructure as a service (IAAS), Platform as a service (PaaS) and Software as a service (SaaS). While edge computing works at the verge, in cloud computing it works at the bottom and in IoT services it works upside.
For data storage and computing resources, via the internet, we can say that cloud computing is an on-demand access infrastructure. It can deliver the resources over the internet as per your requirements [3]. It is also named the "Pay-as-you-go" service. In earlier days, organizations are storing the data in their own PCs and servers. It was becoming very difficult to manage such large physical and on-premises servers. Cloud computing is the solution to all these kinds of problems. Basically, it allows the shifting of computing from local to remote For data storage and computing resources, via the internet, we can say that cloud computing is an on-demand access infrastructure. It can deliver the resources over the internet as per your requirements [3].
It is also named the "Pay-as-you-go" service. In earlier days, organizations are storing the data in their own PCs and servers. It was becoming very difficult to manage such large physical and on-premises servers. Cloud computing is the solution to all these kinds of problems. Basically, it allows the shifting of computing from local to remote For data storage and computing resources, via the internet, we can say that cloud computing is an on-demand access infrastructure. It can deliver the resources over the internet as per your requirements [3].
It is also named the "Pay-as-you-go" service. In earlier days, organizations are storing the data in their own PCs and servers. It was becoming very difficult to manage such large physical and on-premises servers. Cloud computing is the solution to all these kinds of problems. Basically, it allows the shifting of computing from local to remote For data storage and computing resources, via the internet, we can say that cloud computing is an on-demand access infrastructure. It can deliver the resources over the internet as per your requirements [3]. It is also named the "Pay-as-you-go" service. In earlier days, organizations are storing the data in their own PCs and servers. It was becoming very difficult to manage such large physical and on-premises servers. Cloud computing is the solution to all these kinds of problems. Basically, it allows the shifting of computing from local to remote

3. APPLICATIONS OF IOT

- **Smart homes and buildings.**

The use of IoT is advancing in day-to-day activities of home, household devices in smart home can be controlled and monitored from distant area. All these devices are connected through internet using proper architecture and standard protocols thus by making a home Smart Home. [4] layered architecture is introduced by Kang Bing et. al., IoT devices can automate tasks like lighting control, temperature regulation, and appliance management, creating a more comfortable

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

and energy-efficient living environment. The smart home system is divided into three layers: application layer, network layer, and sensing layer.
IoT devices can automate tasks like lighting control, temperature regulation, and appliance management, creating a more comfortable and energy-efficient living environment

- **Industrial IoT (IIoT) in manufacturing and supply chain.**

IoT in industrial sector is behind the 4th industrial revolution, in which manufacturing sector is widely influenced by cyber physical systems, IoT and cloud-based design. Earlier product development was time–consuming and more dependent on labors, but now modern manufacturing technologies uses cloud computing and smart technologies to efficiently use time and services in more economical ways. That helps in analyzing and rectifying failures and its causes.[5] As far as the benefit of Manufacturing 4.0 revolution is concerned the IoT processes big data in which hardware and software are connected with predictive maintenance. We can see that:

- Supply chain organization involves the coordination and management of activities, information, and resources between an organization and its suppliers to deliver a product to the final customer.
- It includes various stages such as raw material procurement, logistics, parts suppliers, components suppliers, and module/system suppliers.
- Raw material procurement involves obtaining the necessary products and semi-products
- for production. Logistics chain ensures the smooth flow of materials throughout the supply chain, requiring capabilities, customer service, and a strong safety record.
- IoT components such as sensors, actuators, embedded systems, and Bluetooth-enabled devices are connected to each other using the cloud as a platform.
- IoT in supply chain management offers benefits such as industrial optimization, safety, interoperability, and agile workflow.
- Challenges in IoT implementation in the supply chain include data security and privacy concerns, maintaining data standards, complexity in business models, and high upfront investment.
- IoT enables constant communication and collaboration between suppliers, manufacturers, and consumers, leading to improved efficiency and customer satisfaction in the supply chain.

Smart Cities: IoT can optimize traffic flow, monitor air quality, and manage waste collection in urban areas, leading to a more sustainable and efficient infrastructure.
Agriculture: IoT sensors can monitor soil conditions, moisture levels, and crop health, allowing for precision agriculture techniques that improve yield and resource management.
Healthcare applications: Wearable devices and sensors can track vital signs, monitor chronic conditions, and remotely assist patients, improving healthcare delivery and preventative care. IoT in various health care service including equipment facilitate patients, doctors and administration, these applications of IoT are used in real-time care of patient sickness and emergency cases. The main objective of the sensors in healthcare services is to control, monitor, warn, regulate and track the activities of the patients. [6]**.**

Smart watches earlier were meant for games, entertainment and other activities but now by multiple applications from the manufacturers such as Samsung, Google and Apple one can keep a check on his/her blood pressure, ECG, respiratory diseases.[7] Along with this, other health-related activities like medication reminder, movement reminder, running, steps count, sleep cycle etc can also be tracked. [8] The various wearable healthcare devices are:

- Mask
- Wrist bands
- Wrist watches
- Electronic tatoos
- Teeth Sensor
- Smart lenses

4. SECURITY AND PRIVACY ISSUES WITH IOT

The IoT technologies faces various issues and challenges due to security flaws. The main target of attackers are nodes which are comprised of sensors, actuators etc. attackers tend to exploit these services by employing self-generated codes. The factors such as low battery power, fake node , jamming, tampering etc are the most common attacks [9].

- **Security and privacy concerns**: IoT systems are vulnerable to various security issues and attacks, that needs to be checked at each layer of IoT protocol. For this purpose we examine these security issues and identify the threats associated which can be manifested at each coating of IoT architecture. [10]

The security challenges, issues in IoT are discussed below:

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

Application Layer

- Data Protection and its recovery, phising attack.
- Reliablity and Clone attack.
- Security parameters are Data privacy and access Control.

Middleware Layer

At this layer data is processed using intelligent decision and authintication so as to minimize malicious attack. The main objective is to maintain integrity and Confidentiality.

Network and Perception Layer

- The security challenges are to safeguard IoT devices from DoS attacks, altered or routing information and spoofing.
- Cryptographic Algorithm and Key management authentication issues are there which are needed to solve authentication and confidentiallity problem of data .

At perception layer attackers want to use their own code and exploit nodes. That ultimately reduces the functionality of IoT devices.

- **Interoperability and standards.** In IoT various entities are interconnected for performing a task and thus formulate inter working connection between users, devices and information resources [11] . Interoperability is very essential for completing the task by keeping in mind data protection and privacy to prevent malicious activities. The many organizations International Organization for standardization, Union and Engineering Task force, Internet Engineering etc performed studies on interoperability and standards which have been useful in maintaining interoperability and security.
- **Scalability and reliability**

Scalability is defined as the ability of device to adapt changes and meet the needs of the people [12] through some steps using which we may make network or system scalable. The types of scalabilities that can be used are Vertical and Horizontal Scalability.

Vertical Scalability: In vertical scalability capacity of hardwa re and software are increased using various resources like memory, storage and processing power.

Horizontal Scalability: In this method the load of the server is decreased instead of increasing server capacity by adding instances to an existing server.

- **Data management and analytics:** The process to optimize the IoT services by analyzing large amount of data is known as data analytics. To achieve these objective data analytics is used with artificial intelligence (A.I.) and deep learning (D.L.). Data management acts as a layer between the things that generates data and one that analyses the data by accessing it through resources.

5. IOT PLATFORMS AND FRAMEWORKS

A group of standards, tools, and protocols that offer a particular framework for building and deploying Internet of Things services and applications.

- **Overview of major IoT platforms (e.g AWS IoT, Microsoft Azure IoT, Google cloud IoT).**

The IoT platform can be classified as theoretical IoT Platform and cloud based IoT Platform. [13] Theoretical IoT platform providing model that support multiplexing and safety when actuators can cause harm. Data association is reliable with new inference techniques and confidential architectural design.

IoT is in early phase of development so all its platform should be able to provide experimentation facilities.[14] There are 16 cloud based IoT platform and services available.

- creating knowledge and big data (real-time data

behaviors,

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

Open-source IoT frameworks.

Open MTC is an open-source, cloud-enabled Internet of Things platform that includes crucial parts that allow back-end platform connectivity to other platforms. The Front-End's Core Features and Connectivity Components, the Front-End and Back-End's Connectivity Component, and their connectivity together provide functioning between IoT devices and middleware.

An open-source IoT platform that follows the IoT reference architecture is called Site Where. The devices can communicate with the platform using a variety of protocols because of the use of a gateway. The Site Where Tenant Engine, comprised of the Device Management and Communication Engines, powers the platform's primary features.[15]

6. KEY FINDINGS

The key findings [9]of literature review done so far is listed below:

(a) Security challenges and issues:

- RFID security problems
- Node security (fake node, mass node and node capture)
- Data integrity and encryption in wireless sensor network(WSN)
- Access of data and its authentication.
- Distributed denial of services.

In context to assessing smart city development and security, block chain are integrated with IoT for smart devices [16], Oracevic et al. discussed analysis of security issues and corresponding solutions for it[17]. The analysis of various layers of IoT and security issues while handling risks is also discussed [18]. Cryptographic mechanism for security of IoT is analyzed by Miraz et al.[19]. Vorakulpipat has described depth analysis of IoT architecture and applications[20]. While integration of IoT architecture and blockchain and their assessment, feasible use of these integrated structure for leveraging IoT security issues are well explained by Roy et al[21].

How IoT comes out of all these major problems with solutions[22]:

- The problem of per device identification can be resolved using Lpv6 hardware address.
- The solution to the problems originated from authentication of various devices in real time can obtained by handshake process or public key cryptography.
- SQL lite may help in data management which is preloaded.
- For fast communication between devices RFID tags can be used but it has some limitations like prone to hacking.
- Many loophole are there in authentication and control of data technology is still developing and system is vulnerable to man in the middle attacks. These loopholes are need to be corrected.
- Node security is a major issue they are needs to be improved and developed here encryption needs to be fast.

7. FUTURE TRENDS

The objective to achieve security and privacy in IoT, good quality of research and innovations are needed. The area in which research required are Scaling, architecture, big data use and analysis, openness and security issues. Key area of research is scaling of large number of devices connected to perform function using IoT, its architecture which supports simple ways for connectivity, communication and controls. The storage capacity and transmission of data, these are the areas where there is scope for research.

8. CONCLUSION

IoT will play a key role in coming generation because of its capabilities to sense and actuate, which makes it unique. It is a bond between real and virtual word which connects human to machine as well as machine to machine. While using IoT security and privacy issues are needed to be taken into consideration. In this paper IoT, its architecture and framework is discussed and findings of many researchers are marked. How IoT works, its connectivity and vulnerability to attacks, its solution are mentioned. The future of IoT is very bright and in order to maintain a pace with smart devices the traditional network protocols and security mechanism needs to be upgraded.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 3, March 2025
DOI 10.17148/IMRJR.2025.020302

REFERENCES

[1] S. Madakam and R. Ramaswamy, "Smart Homes (Conceptual Views)," *2nd Int. Symp. Comput. Bus. Intell. 2014*, 2014.
[2] "Britannica."
[3] V. Gandhi and C. K. Kumbharana, "V. Gandhi, and C. K. Kumbharana. 'Comparative study of Amazon EC2 and Microsoft Azure cloud architecture.' International Journal of Advanced Networking & Applications (2014): 117-123," *Int. J. Adv. Netw. Appl.*, pp. 117–123, 2014.
[4] J. P. Gabhane, Ms. S. Thakare, and Ms. M. Craig, "Smart Homes System Using Internet-of-Things: Issues, Solutions and Recent Research Directions," *Int. Res. J. Eng. Technol. IRJET*, vol. 04, no. 05.
[5] A. R.G., S. Oswal, and J. Subramanian, "Industrial IoT in Manufacturing and Supply chain Management," *Int. J. Sci. Eng. Appl. Sci. IJSEAS*, vol. 6, no. 9, 2020.
[6] M. S.Alkahtani, F. Khan, and W. Taekeun, "Application of Internet of Things and Sensors in Healthcare," *Susanna Spinsante Acad. Ed. Biswanath Samanta Acad. Ed.*, 2022, doi: 103390/s22155738.
[7] Y. Zhang, J. Cui, K. Ma, H. Chen, and j Zhang, "A wristband device for detecting human pulse and motion based on the Internet of Things. Measurement. 2020;163:108036. doi: 10.1016/j.measurement.2020.108036.," *Measurements*, 2020, doi: 10.1016/ j.measurement.2020.10806.
[8] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. . 2018;78:641–658. doi: 10.1016/j.future.2017.02.014," *Future Gener Comput Syst*, vol. 78, pp. 641–658, 2018, doi: 10.1016/j.future.2017.02.014.
[9] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and Kashif Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context.," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, pp. 2161–5748, 2022.
[10] A. Bahalul H and S. Tasmin, "Security Threats and Research Challenges of IoT-A Review AKM Bahalul Haque* and Sonia Tasmin," vol. 1, no. 4, pp. 170–182, 2020.
[11] E. Lee, Y. Seo, and S.-R. Oh, "A Survey on Standards for Interoperability and Security in the Internet of Things," vol. 23, no. 2, 2021.
[12] R. D. Rosa Righi, M. Gomes, and C. A. Da Costa, "Internet of things scalability: Analyzing the bottlenecks and proposing alternatives".
[13] M. Zdravković *et al.*, *Survey of Internet-of-Things platforms*. 2016.
[14] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, and N. Mitton, "A Survey on Facilities for Experimental Internet of Things Research., 2011, 49 (11), pp.58-6," *IEEE Commun. Mag. Inst. Electr. Electron. Eng.*, vol. 49, no. 11, pp. 58–67, 2011.
[15] D. Lau, J. Liu, B. Nandy, M. St. Hilaire, and C. S. Yang, "A cloud-based approach for smart facilities management," *Conf. Progn. Health Manag. PHM IEEE*, 2013.
[16] A. Dorri, S. Kanhere, S. Judrak, and P. R and Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home.," in *IEEE conference on pervasive computing and communications workshops(PerCom Workshop)*, 2017, pp. 618–623.
[17] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in Internet of things," in *ISNCC*, May 2017, pp. 1–6.
[18] M. M. Ahmed, M. A. Shah, and A. Wahid, "IoT Security: A layered approach for attacks & defenses.," in *(C)mTech)*, 2017, pp. 104–110.
[19] M. H. Miraz and M. Ali, "Blockchain enabled enhanced IoT ecosystem security.," presented at the International Conference for Emerging Technologies in Computing, Springer Cham, 2018, pp. 38–46.
[20] C. Vorakulpipat, "Recent challenges, trends and concerns related to IoT Security : An evolutionary study.,"
[21] S. Roy, M. Ashaduzzaman, and A. R. Chowdhury, "Blockchain for IoT security and management: Current prospects, challenges and future directions.," presented at the 5th International Conference on Networking , System and Seccurity IEEE, 2018, pp. 1–9.
[22] S. Alampalayam Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things : Challenges, Solutions and Future Directions," 2016.