Journal of Futuristic Sciences and Applications
Vol. 7(1), Jan-Jun 2024, pp. 56-64
doi: 10.51976/jfsa.712408
www.gla.ac.in/journals/jfsa

Analysis of Implementation Areas of IOT with Security Features

Dhirendra Pratap Singh and Anurag Kumar***

ABSTRACT

Small wearables to large industrial systems—the Internet of Things (IoT) is radically altering modern living. Infrastructure and amenities that are ubiquitous, dependable, high performing, efficient, and scalable are needed for the Internet of Things. IoT services work with a wide range of devices, from simple to complicated technologies, and communication occurs through a variety of networks. Cloud computing is the most significant aspect of the Internet of Things since it not only connects servers, but it also analyzes critical data acquired from sensors while also providing sufficient storage space. Further organisation and resale data will be required in the near future to finish this attribution. Certain Internet of Things (IoT) applications facilitate process automation and allow non-living physical things to function without the need for human interaction. Internet of Things (IoT) applications in the industrial sector could boost productivity and enable more extensive networks of communication between workers and equipment. Ultimately, this would enable a greater number of competitive businesses to enter the market, which would improve quality control and reduce losses. This article discusses many technologies risks as well as their advantages and the many uses of IoT, including smart towns and cities, medical care, and industry.

Keywords: *IoT, Security, RFID, WSN, Application, Radio frequency identification.*

1.0 Introduction

Now a days, the most concern topics between all academicians and research specialist is Internet of Things (IoT). It allows all objects /things available in our surrounding are to be connect with each other without involvement of mankind. IoT is a rapidly growing field of study with lots of untapped potential. Thanks to its boundless innovation, it is on the verge of converting the internet’s existing shape into a modern and interconnected one. The number of internet-connected gadgets is increasing every day, and connecting all with IoT, whether by wire or wireless, will ensure a continuous flow of data [1]. In year 1982, IoT was established when a customized Coca-Cola machine was connected to the Internet and could detect how many drinks were left and whether they were cold or not. The phrase “pervasive computing” was used by Mark Weiser in 1991 to characterize the first modern concept of the IoT.

2.0 Threats of Internet of Things (IoT)

IoT services can be used with a broad variety of devices, from simple to complicated machinery, and communication is done through a number of networks.

**Corresponding author; Professor, Department of Mechanical Engineering, SR Institute of Management and Technology, Lucknow, Uttar Pradesh, India (E-mail: Dheerendra.19732pratap@gmail.com)*

***Assistant Professor, Department of Computer Science & Engineering, Bhudelkhand University, Jhansi, Uttar Pradesh, India*

IoT services work with a wide range of devices, from simple to complicated technologies, and communication occurs through a variety of networks [2].

2.1 Data life-cycle security from end-to-end

To ensure data security in the IoT environment, end-to-end (E2E) data security across the complete IoT service should be offered. Data is generated from a wide range of sources and disseminated at randomly through an open network such as the internet [3]. As a result, throughout the data life cycle, the data protection framework must be capable of controlling and measuring sensitive data protection information.

2.2 Secure things orchestration

The Internet of Things connects things in a natural manner, and the objects that are connected change with time. The linked gadgets should be capable of maintaining the required level of security in this case. Local sensing devices used in the home, for example, should communicate securely with one another and be kept safe to allow multi-thing cooperation. Furthermore, when interacting with mobile devices, they all should follow the same security policy.

2.3 Multi-level things security platform

There are several different sorts of devices and platforms in IoT environments, ranging from small sensors to smart phones. As previously noted, a security concern in one item can rapidly spread to certain other items, making multi-thing safety challenging to secure [4]. As a consequence, each item must have a secure SW execution environment. Because everything has different abilities, such as computer power and memory size, the same infrastructure security cannot be applied to all. As a result, security mechanisms should be built that give the right degree of security based on object abilities and responsibilities.

2.4 Security and privacy visible/usable

Mis-configuration by users is the source of many security and privacy flaws. On the other hand, ensuring that users are aware of complex security/privacy policies or processes will be incredibly difficult and unrealistic. As a result, technologies that make creating and enforcing security and privacy policies simple are essential.

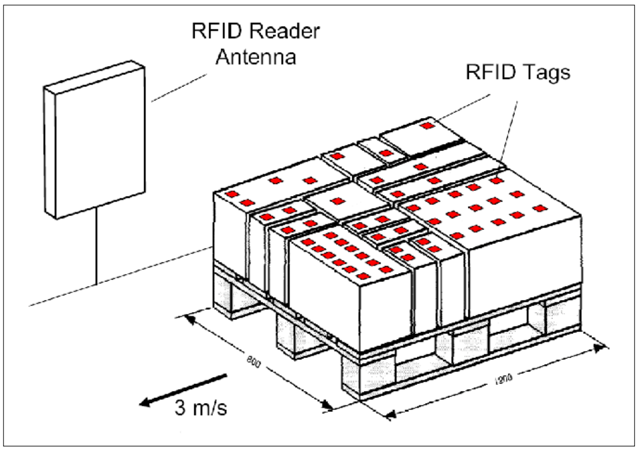
3.0 Technologies

In order to collect data about which autonomous actions may be taken, a number of unique and successful ways must be utilized in the building of widely used computer systems in which electrical things can be detected instantly and can think and interact with other objects [5]. The only way to do it is to use open source code. To develop products that can recognize and communicate with one another, many ways are combined. This section includes features: We look at how technology may aid large-scale undertakings. The Internet of Things (IoT) is becoming increasingly popular.

4.0 Radio Frequency Identification (RFID)

RFID (Radio Frequency Identification) is a technology that identifies objects based on their unique frequency. Because of its small size and low cost, it may be incorporated into any object. It’s an active or passive transmitter microchip in the form of an adhesive sticker, depending on the specific needs. Because tags are continually active and so release energy, they have a batteries connected to them [6]. Passive tags are only engaged when signals are activated, but active tags are only active when they are ready to convey data. Active RFID tags are more expensive and more extensively used than passive RFID tags When triggered by the generation of any relevant signals, a System comprises of readers and linked RFID tags that broadcast the object's identification, position, or any other parameters about the object. The specified object-related sent data is received by the Readers. Before being delivered to the CPU, the data is verified using wireless signals. Fig.1 shows the RFID scenario.

Figure 1: RFID Scenario



RFID frequencies are split into four frequency ranges, that are given below, depending on type of application:

1. Frequency is low (135 KHz or less)
2. Frequency is High (13.56MHz)
3. Ultra-High Frequency (862MHz 928MHz)
4. Microwave Frequency (2.4G , 5.80)

4.1 Wireless Sensor Network (WSN)

WSNs are multi-hop bi-directional sensor that are built up of numerous nodes that are distributed across a sensing area and are each linked to one or more information sensors. Multi-hop communications is used by the perception layer. Each sensor contains an antenna, microcontroller, and sensor interface circuit, and functions as a transceiver. Nonetheless, as a component for communication, actuation, and sensing with a power source for harvesting energy that might be a battery or other type of power generation [2], an additional proposal has been offered [7]. A memory unit is a type of memory device which can store data. Temperature, humidity, speed, and other object-specific data are collected by the sensor network. After that, it's off to the processing facilities.

Non-internet sensors are those that aren't connected to the internet. New smart device opportunities emerge when network and RFID technologies are intertwined, and numerous methods have been offered to address this. WSNs and RFID Sensor Arrays both have advantages, but WSNs have a considerably greater range and peer-to-peer communication, whilst RFID Sensor Networks have a lower range and asymmetric interaction.

4.2 Cloud computing

The internet appears to be the only technology capable of processing and storing all of the data, By 2022, millions of gadgets are projected. It’s a pervasive computing technique that connects a large number of machines into a single cloud service, enabling resource sharing and access from any location and at any time [8]. Cloud computing is the most significant aspect of the Internet of Things since it not only connects servers, but it also analyzes critical data acquired from sensors while also providing sufficient storage space.

4.3 Optical technologies

The Internet of Things could be transformed by recent breakthroughs in optical technology, Li-Fi and Cisco’s BiDi optical technology, for example. Li-Fi, an epoch-making Visible Light Communication (VLC) technology, will provide superior connectivity at a higher bandwidth for IoT-connected devices. BiDi technology, on the other hand, provides a 40G ethernet cable for transmitting huge volumes of data from a variety of IoT devices.

4.4 Networking technologies

This method allows to make smaller, more accurate clones of related items. It makes it easier to develop nanometric devices that can function as sensors and devices in the same way that conventional devices do, hence eliminating the need for conventional devices. The resulting network is called the Internet of Nano-Things, a novel networking paradigm comprised entirely of nano-components [9].

4.5 Micro-electro-mechanical systems technologies (MEMS)

MEMS are electronic and mechanical elements that work together to enable a variety of applications, including detection and actuator. In the form of transducers and accelerometers, they are currently widely available. MEMS paired with Nano technology is a low-cost solution to improve IoT communication systems, with added features including smaller sensors and controls, embedded ubiquitous desktop computers, and a wide frequency range.

In the form of transducers and accelerometers, they are currently widely available. MEMS paired with Nano technology is a low-cost solution to improve IoT communication systems, with added features including smaller sensors and controls, embedded ubiquitous desktop computers, and a wide frequency range.

5.0 Application Areas

There are numerous IoT application areas, and the most popular application sectors are based on currently available technology solutions [10]. Several important factors have an impact on the growth of particular IoT application areas, including:

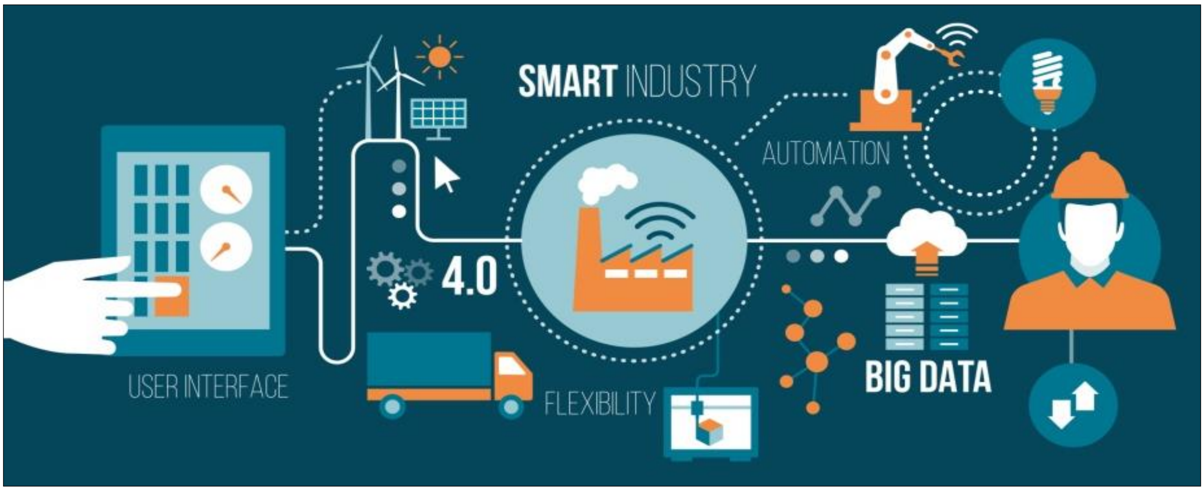
- Electronic hardware advancements in broad
- Software solutions are available, as well as a user-friendly environment.
- Solutions for data gathering and sensing technology
- Network quality, or network connection and infrastructure, is a term used to describe how well a network works.
- Adequate power supply for IoT system production activities.

The editorial will then go on to look at some of the most important IoT application areas, as well as noteworthy advancements and present issues.

5.1 Industry and the internet of things

Industrial applications of Internet of Things (IoT) technology would increase efficiency while also allowing for greater communication networks between employees and machinery. Finally, this would allow more competitive enterprises to come into the market, resulting in better quality control and lower losses. A significant component of developing comprehensive and successful management would be the creation, design, and deployment of a variety of sensors in industrial applications. More study is needed to guarantee that technology is properly incorporated into industry, as well as to gain a deeper understanding of how IoT technology may be used to help diverse industries. The IoT in Industry working mechanism is depicted in Figure 2.

Figure 2: IoT in Industry



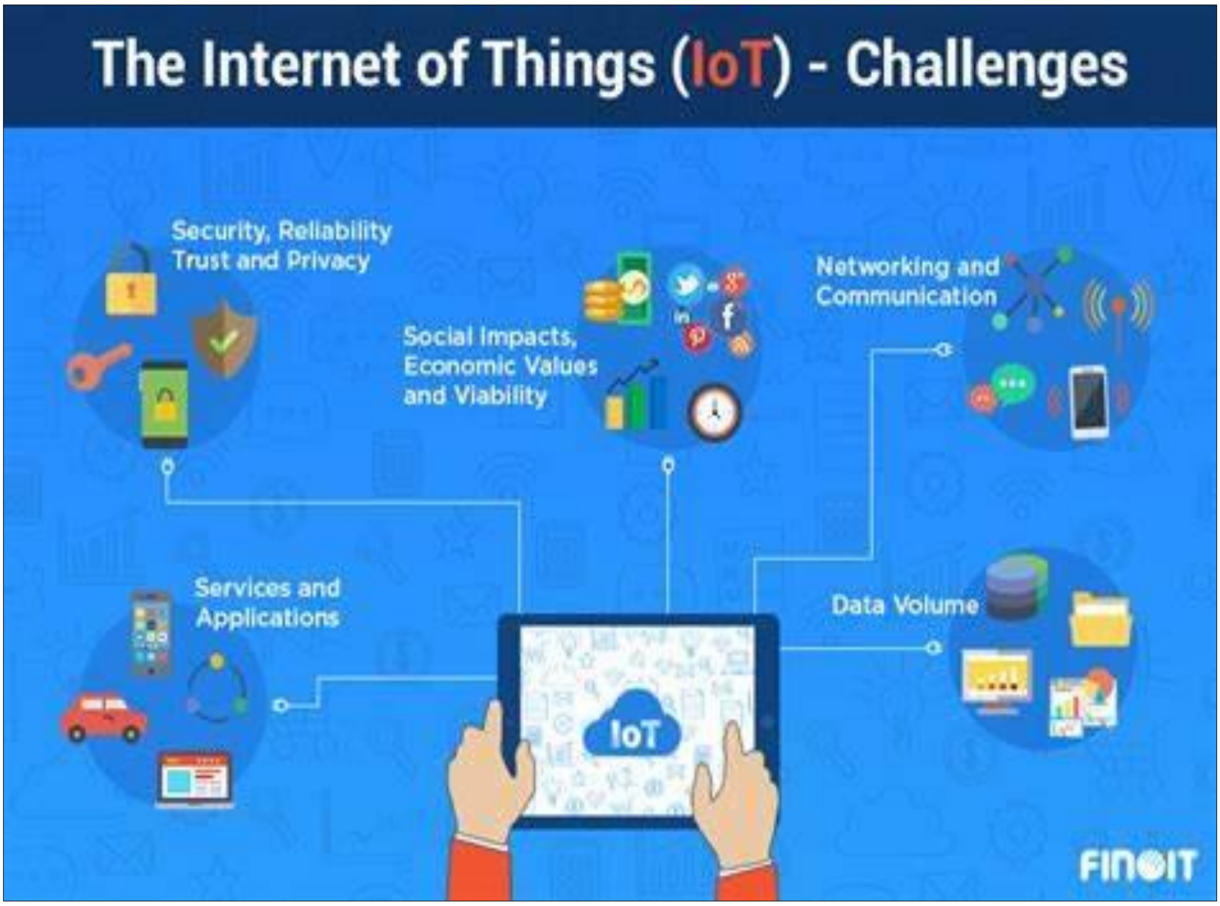
5.2 IoT for smart cities

The smart city concept’s usage of IoT technology is critical for tackling the previously listed infrastructural challenges in cities, which are linked to current population development. Future-looking city IoT technology enables the use of a wide range of devices, enhancing the quality of city life and lowering the cost of many routine activities such as transportation, security (surveillance), monitoring devices, smart energy systems, smart water management, and so on. Information will be examined with the help of a range of sensing devices in order to deliver effective solutions.

In smart cities, early detection of various faults or infrastructure flaws will be a crucial benefit of IoT technology (such as traffic congestion, electricity supply, water shortages, security events, and so on). Many sensors are installed in smart cities, and they communicate to a range of other devices via the internet, giving users with information about parking spots, malfunctions, electrical problems, and a variety of other concerns [11]. This technology could be used in smart warehouses, smart healthcare transportation, smart grids smart waste management, smart communities, and other smart city projects.Fig.3 shows Challenges in IoT.

The most pressing challenges include, among other things, the proper integration of various sensing technologies, the development of adequate infrastructure, population knowledge, and sustainable research, such as impact on the environment. According to smart city managers, the use of Internet of Things (IoT) technology in smart houses improves the life quality in residences while also providing creative and appealing innovative solutions. Time management, which is a vital feature in our present financial paradigm, could save money and energy. Several control systems are available within the smart house concept, allowing for the successful integration of renewable energy technologies in homes and their efficient balancing.

Figure 3: IoT Challenges


The Internet of Things (IoT) - Challenges
Security, Reliability Trust and Privacy
Social Impacts, Economic Values and Viability
Networking and Communication
Services and Applications
Data Volume
IoT
FINOIT

5.3 IoT in healthcare

The e-health concept has shown one of the most problematic areas of IoT technology application in the healthcare sector. Improved patient security and care may result in a rise in healthcare system service quality, which may lead to an increase in patient life expectancy, thanks to IoT support (primarily the collection of patient health data).

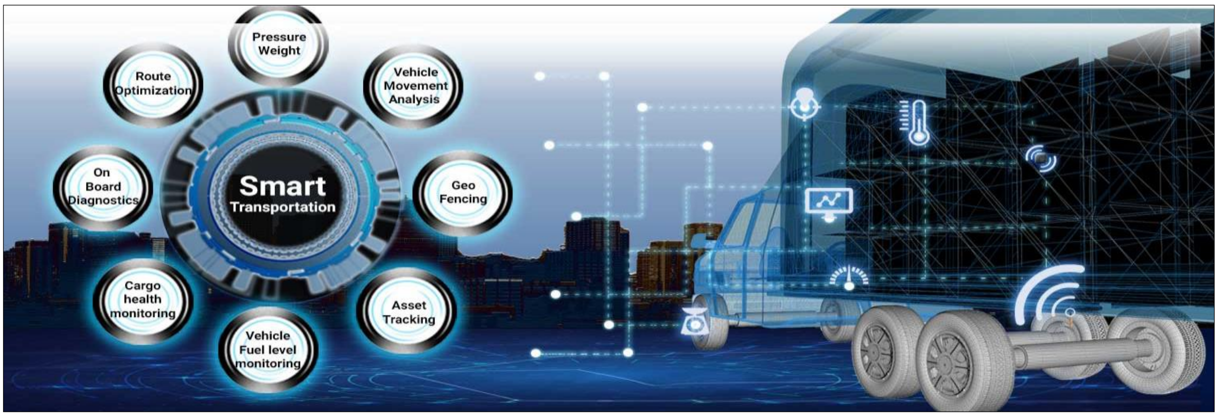
Intelligent health devices have a lot of potential in terms of measuring a variety of vital and valuable human functions, such as heart rate, body temperature, and movement monitoring, to mention a few. Another intriguing concept that could be realized with the right IoT goods and infrastructure is remote monitoring. In general, it may be possible to forecast a variety of symptoms and prevent potentially fatal illnesses and diseases [12]. The elderly may benefit from monitoring their general health and nutritional status, which might be supported by IoT devices.Fig.4. shows IoT in healthcare.

Figure 4: IoT in Healthcare

5.4 IoT in transportation

The approaching ban on gasoline vehicles, as well as the subsequent search for alternative transportation technologies like as hydrogen-powered cars, will have a significant impact on future transportation system architecture. The idea of the internet of automobiles has recently surfaced, showing the IoT's potential in this vital industry. The most significant application area for the smart automobile (vehicles) idea is the Internet of Things (IoT). The smart car idea takes into account the utilization and optimization of a variety of internal vehicle functions made possible by IoT technology. The smart car gathers information and associates it with important operating features such as tyre pressure, fueling, early detection of possible faults, and regular maintenance indicators, among others. In general, a well-targeted adoption of IoT technology can increase customer service and value, increasing automakers' competitiveness. Fig.5. shows IoT in transportation.

Figure 5: IoT in Transportation



6.0 Conclusion

IoT services are compatible with a vast array of devices, spanning from basic to sophisticated technology, and communication takes place over multiple networks. The Internet of Things' most important feature is cloud computing, which links servers and analyses vital data collected from sensors in addition to offering enough storage. Applications of the Internet of Things (IoT) in industries such as manufacturing have the potential to increase output and provide wider networks of communication between personnel and machinery. In the end, this would make it possible for more rival companies to join the market, which would enhance quality assurance and lower losses. WSNs and RFID Sensor Arrays both have advantages, but WSNs have a considerably greater range and peer-to-peer communication, whilst RFID Sensor Networks have a lower range and asymmetric interaction. Despite its many benefits, the internet of thing has a lot of problems, particularly in terms of data security. Addressing these concerns, as well as ensuring the privacy and security of IoT goods and services, should be a top priority. Several technology and application areas are discussed in this article, namely IoT in Industry, Intelligent Buildings, Healthcare, and Transport.

Refernces

[1] Atlam, Hany F., and Gary B. Wills. “IoT security, privacy, safety and ethics.” *Digital twin technologies and smart cities*. Springer, Cham, 2020. 123-149.

[2] Alfandi, O., Khanji, S., Ahmad, L. *et al.* A survey on boosting IoT security and privacy through blockchain. *Cluster Comput* 24, 37–55 (2021). https://doi.org/10.1007/s10586-020-03137-8.

[3] Vaishali Yadav and V. K. Tomar, “A Low Leakage with enhance write margin 10T SRAM cell for IoT applications” published in oceedings of “International Conference on Micro/Nanoelectronics Devices, Circuits and Systems (MNDCS-2021), National Institute of Technology, Silchar, 30-31 January 2021. pp 201-211 Print ISBN: 978-981-16-3766-7, https://link.springer.com/chapter/10.1007/978-981-16-3767-4_19,Editors- Dr. Trupti Ranjan Lenka, Prof. Durgamadhab Misra, Prof. Dr. Arindam Biswas Publisher: Springer Singapore

[4] Thakurendra Singh and V. K. Tomar, “Post Simulation of High Speed Sense Amplifiers using 45 nm CMOS Technology Used in IOT application” 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC 2022) held during 21st -22nd January, 2022 organized by Department of Electrical Engineering, GLA University, Mathura, India DOI: 10.1109/PARC52418.2022.9726536

[5] 3. K. K. S. Gautam, R. Kumar, R. Yadav and P. Sharma, “Investigation of the Internet of Things (IoT) Security and Privacy Issues,” *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2023, pp. 1489-1494, doi: 10.1109/ICIRCA57980.2023.10220814**.**

[6] M. S. Rajan, J. R. Arunkumar, A. Ramasamy and B. Sisay, “A comprehensive study of the Design and Security of the IoT layer Attacks,” *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatre, India, 2021, pp. 538-543, doi: 10.1109/ICCES51350.2021.9489235**.**

[7] J. Singh, G. Singh and S. Negi, “Evaluating Security Principals and Technologies to Overcome Security Threats in IoT World,” *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, 2023, pp. 1405-1410, doi: 10.1109/ICAAIC56838.2023.10141083.

[8] Vivek Kumar and V. K. Tomar “A Comparative Performance Analysis of 6T, 7T and 8T SRAM Cells in 18nm FinFET Technology”, Presented in International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC 2020) on 28-29 Febuary,2020 at GLA University, Mathura .(PP-329-333) ISBN No- 978-1-7281-6576-9, DOI: 10.1109/PARC49193.2020.236620.

[9] V. Obarafor, M. Qi and L. Zhang, “A Review of Privacy-Preserving Federated Learning, Deep Learning, and Machine Learning IIoT and IoTs Solutions,” *2023 8th International Conference on Signal and Image Processing (ICSIP)*, Wuxi, China, 2023, pp. 1074-1078, doi: 10.1109/ICSIP57908.2023.10270935**.**

[10] N. Tewari and G. Datt, “A Systematic Review of Security Issues and challenges with Futuristic Wearable Internet of Things (IoTs),” *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, Tashkent, Uzbekistan, 2021, pp. 319-323, doi: 10.1109/ICTAI53825.2021.9673353.

[11] Nižetić, Sandro, et al. “Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future.” *Journal of Cleaner Production* 274 (2020): 122877.

[12] A. Sindgi, M. Adil and P. Chaudhary, “Automated Security Evaluations for IoT Deployments,” *2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC)*, Greater Noida, India, 2023, pp. 812-816, doi: 10.1109/PEEIC59336.2023.10451350**.**

[13] D. R. M S, R. A and A. Agarwal, “The Innovative Cloud Security Environment for Data Privacy,” *2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC)*, Greater Noida, India, 2023, pp. 748-751, doi: 10.1109/PEEIC59336.2023.10450434**.**

[14] Shukla, Aasheesh. “Optimal Multiple Access Scheme for 5G and Beyond Communication Network.” *International Conference on Information and Communication Technology for Intelligent Systems*. Springer, Singapore, 2020.