Phoenix: International Multidisciplinary Research Journal
Vol 3, No. 2, April-June, 2025
ISSN: 2583-6897

IOT SECURITY AND PRIVACY CHALLENGES: A REVIEW

B. Sankaraiah
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: Shankar61186@gmail.com
Vemula Nikitha
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: nikitha479@gmail.com
Syed Abdul Haq
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: abdulhaq007@gmail.com
Dr. Syed Umar
Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: syedumar@mrec.ac.in

Abstract— The Internet of Things (IOT) aims to transform our surroundings—including our houses and flats, places of employment, and cars—into something smarter, more measurable, and more hospitable. Voice technology can make it easier to play music, create countdowns, or receive information. It is easier to monitor actions both inside and outside, as well as to recognize and engage with visitors, thanks to surveillance cameras. Intellectual light bulbs could perhaps give the illusion as if we are parents' house even when we are not, but instead smart devices can help us warm heat our homes before we arrive. When we look outside the house, sensor nodes can tell us how noisy, frustrating, or contaminated our enviroment But several of these developments could have a big impact on our right to privacy. Users are likely to interact with internet-enabled gadgets for the first time through home automation, another market where the main tech companies are engaged in strong competition. Examples include smart sensors, smart lighting fixtures, camcorders, smart thermostats, and the smart fridges. The issues related to the Internet of Things, health, and privacy are discussed in this paper, along with suggestions for IoT solutions.

Index Terms—Internet of Things (IOT), Security and Privacy Challenges, Data-Sharing

I. INTRODUCTION

"Internet of Things" (IoT) [1] offers enormous potential for creating creative, intelligent applications in almost every industry. This is mostly because it can do situated sensing (enabling, for example, to gather data about natural occurrences, medical factors, or user habits) and provide them with services that are based strategies to their needs. Regardless of the application area, these apps aim to improve daily life and will have a significant impact on the economy and society. Hey would also cover a wide range of topics [2]. Such as logistics, personal, social, and societal issues.

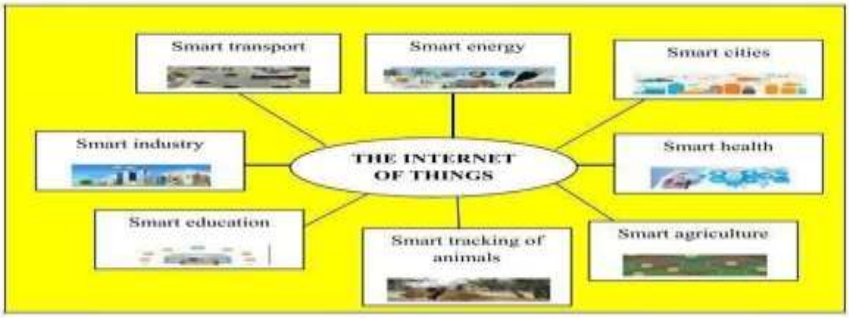

Figure 1: The applications of IOT

The different applications [3] can be divided into three primary categories: industrial, smart city, and health and well-being considering that some applications are shared, no domain is completely separate from the others; rather, there is some overlap. One example is inventory tracking, which is widespread in

both the industrials and health care domains because it may be used to monitor containers containing foods, but it can also be used to monitor pharmaceutical medicine supplies. It should be noted that not all Implementations have reached this very same level of maturity. Some application, usually the most basic [4] and user- friendly, is already a part of our daily lives. Many others are still in the testing stage since they call for greater coordination between the different actors. Finally, others are still in the early stages and are more futuristic. The most well-known applications for each domain are described in the section that follows.

Industrial Domain: All industrial activities that involve business and financial transactions between organizations, companies, and other entities can benefit from the IoT. Typical examples include logistics, manufacturing, process monitoring, the service industry, banking, financial regulatory bodies, intermediaries, etc.

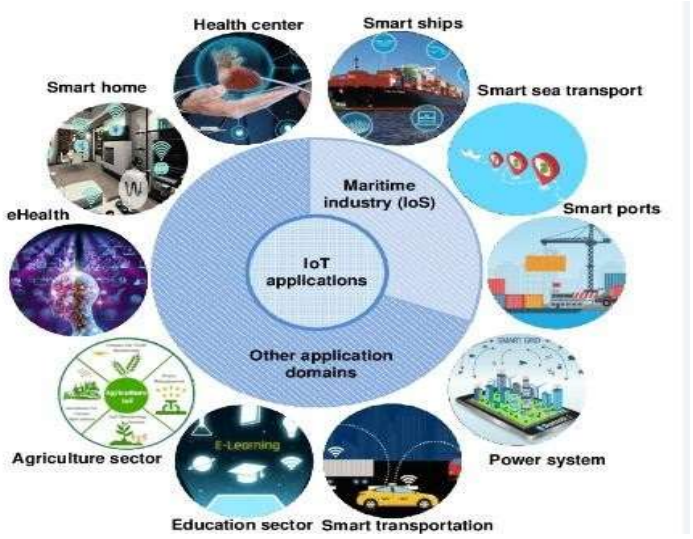

Figure 2: IoT application domains and related application

Logistic and product lifetime management: Logistics and supply chain management are prime examples of an industrial Internet of things applications. Whether it's clothing, furniture, and equipment, food, or liquids, RFIDs may be affixed to things and used to identify materials and goods. By giving correctinformation of the existing inventory and lowering inventory inaccuracies, their use aids in the management of warehouses and retail spaces as well as simplifies the inventory. It is alsopossible to follow an object's complete lifecycle. For instance, RFID readers put throughout the manufacturing facility enable production process monitoring, and the label may be tracked along the whole distribution chain. Advanced IoT systems that include RFID- enabled products and smart shelves that track things in real time could assist to cut down on material waste, which would lower prices and increase profit margins for both producers andmerchants. For instance, if shelves are only half stocked with goods, sales are predicted to drop by about 8.3% [5] . By accurately estimating the number of things that are required, which may be determined by examining the data gathered by smart shelves, underproduction and overproduction can be reduced significantly. Additionally, product degeneration events can be detected in real-time by sensors, which is crucial for food and beverages. For instance, sensors may regularly monitor the temperatures and humidity inside of cold storages or other storage facilities to ensure the freshness of perishables (such as fruits, vegetables, and frozen food), and actuators may change these conditions to ensure the best possible food preservation[6]. Additionally, RFID-based authentication procedures may be used to assure product integrity. Intelligent shopping systems are among the IoT applicationsthat are interesting. By tracking users' mobile devices, these systems keep tabs on their spending patterns and assist customers at stores, supermarkets, and malls by offering deals or facilitating quick payments [7].

Agriculture and breeding: Breeding and agriculture may benefit from IoT. In fact, requirements for animal traceability demand constant observation of animal, as well as their motions, in order to quickly alert the proper authorities to any relevant occurrences, such as diseases. Utilizing IoT identification systems, such as RFID and sensors, enables the identification and monitoring of animals as well as the

separation of sick animals from the healthy ones, preventing the spread of infectious diseases With the goal of streamlining animal health certification, regulating trade and imports, and preventing potential fraud, Advanced microchips may record or send information on the animal's body health (e.g., demographic data, veterinarian check, contracted diseases, administered vaccines) (e.g., temperature) [8]. Authorities may confirm the precise amount of animals reported by local breeders through the analysis of collected data and consequently award subsidies. Additional IoT applications include monitoring and managing feed and agricultural production (e.g., presence of OMGs, additives, or melanin) utilizing sophisticated sensor systems. These techniques will guarantee the safety of products made from plants that are meant for both human and animal use.

Industrial processes: Internet of things can provide cutting-edge automobile industry solutions. The real-time diagnosis of vehicles is a crucial application. Pressure, engine data, and utilisation of fuel, position, speed, separation other vehicles, driving time, stops, etc. and driver presence can allbe monitored by specific sensors. The centre system is then informed of the sensed data [9].The wireless identifier technology attached to automotive components can be used to improve arrangement by immediately locating missing elements and keeping track of the history of specific automobile components. Modern transportation networks for both personsand cargo are made possible by the use of IoT technologies. Examples include collecting fares, managing luggage more safely through computerised tracking and sorting, and conducting thoughtful passenger screening. IoT-based smart industrial management systems enable the monitoring of industrial facilities, for example to lower accident rates, particularlyin the case of high-risk facilities (e.g., oil plants, gas plants)

Smart city domain: IoT could improve both the quality of life for people and the environmental sustainability of our cities. The focus is on finding practical methods to enjoy the personal stay while managing energy effectively.

Figure 3: Smart city schematic representation

Smart Grid: A sustainable ecosystem requires effective energy management, and the Smart Grid is a key component in making that a reality. In fact, The development of sources has led to atremendous upgrade of both the traditional electrical power distributions systems and energy distribution. The smart grid is defined as an intelligent electrical transmission system that provides energy flows including both directions, from manufacturers to end users [10]. With contrast to conventional power systems, where n a smart grid, power is supplied primarily bya simple number of fundamental power plants and "wide cast" to final consumers via strong networks of cables, switchgear, and depots; however, manufacturers may also serve as final customers. The grid receives the energy generated by the micro-grids of the customers (such as from solar panels and wind turbines) and controls it correctly through intelligent energy control services before storing it in designated energy storages.

Medical and healthcare: The IoT will have a significant impact on the medical and healthcare industries. Real-time observation of medical indicators and essential functions is possible thanks to advanced sensing

technology (e.g., temperature, blood pressure, heart rate, cholesterol level). The obtained information is subsequently sent using common or specialized communication technologies (such as Bluetooth, ZigBee, Wireless HART, and ISA100) and made accessibleto medical professionals for the purpose of patient diagnosis and health management. Body Area Network (lan (BANs), created by wearables linked together, enable medical professionals to continue monitoring a remote patient outside of the hospital [11].The identification of materials and the identification of medical devices are two other pertinent applications. For instance, the use of smart cards would guarantee reliable tracking of goods to prevent lost or stolen equipment or the insertion of material into a patient during surgery . Smart label usage is crucial for making it easier to inventory medical supplies. Offer this service, HVAC systems, and safety access systems are all examples of effective hospital administration services. The latter relate to digital access control made possible by smart badges (such those fitted with RFIDs) to restrict entry to specific hospitals areas to authority staff only. The hospital would also be furnished with a number of Internet access points, or "totems," which serve as a way for patients to schedule appointments or find out where and when their medical exams will be performed. Smart touch screen terminals will be installed in each bed to give Patients have access to a variety, They have access to TV channels, the internet, and the opportunity to communicate with their relatives. Furthermore, young patients may use them to access educational services supplied by their schools (e.g., online class, access to recorded lessons).

II. LITERATURE REVIEW

Abdel-Basset, Mohamed et al. [2019], Due to the fulminating proliferation of information in recent years, the role of education in spreading knowledge has grown in importance. Meanwhile, the manner that education is organized is changing, requiring that different pupils finish their learning in a variety of ways. As a result, smart learning environments are promoted. It combines a variety of information and communication technologies to speed up the learning process and cater to the needs of various students. Students' learning processes can be improved by continuously seeing and evaluating the states and actions of various students using information sensing devices and information processing platforms to provide feedback onthe various students' learning processes. The Internet of Things promises to greatly alter life, improve people's quality of life, and increase business productivity. The IoT has the potential toenable expansions and enhancements to fundamental utilities in numerous industries while presenting a cutting-edge ecosystem for developing applications through a widely dispersed locally smart network of intelligent items. The quality of education will be improved by implementing the Internet of Things concept in any educational setting because students will learn more quickly and teachers will do their duties more effectively. This essay aims to provide an overview of the fundamental ideas, terminology, traits, technological developments, and difficulties surrounding the Internet of Things. We also provided examples of how the Internet of Things can be used to create intelligent educational processes and to help us make decisions that are critical to our daily lives.

Ortiz, Antonio M., et al. [2014], The Internet of Things (IoT) and social networking sites (SNs) work together to link individuals to the world of cloud computing. In this system, the IoT provides the information from the environment, and the SN provides the connecting element to enable interactions between humans and machines. This article examines the Social Internet of Things(SIoT), a revolutionary model for pervasive computing that goes beyond IoT. Although early research in social-driven IoT have been conducted, they only leverage one or a few SIoT features to enhance a number of particular performance variables. This paper first provides a comprehensive overview of SIoT and essential views. The progression of IoT study from the Intranet of Things to SIoT is then described along with a study of the literature. This paper also discusses enabling technologies, research hurdles, and outstanding topics before suggesting a generic SIoT design.

Algarni et al. [2019], Healthcare information systems (HISs) have been created thanks to developments in wireless technology. In HIS, detectors, wearable’s, and other gadgets keep an eye on a patient's critical statistics. The designated emergency services or the reliable healthcare professionals receive these parameters for examination. The primary concerns are with the security and privacy of vitals during collection and transmission. Therefore, it is crucial to talk about security methods, issues, and demands in HIS. We examine the SHS's methodologies, goals, platforms, and methods. In the beginning, we provide a brand- new classification system for SHS that rates their techniques according to the relevant

domains. The second step is to organize the literature on SHS into categories. Third, we look at the most significant security breaches in SHS and the suggested defenses. We conclude by identifying the open-research challenges in the security and privacy of HIS and outlining future researchdirections.

Sabita khatri1 , Fahad Ahmed Alzahrani et al. [2021], Blockchain can be used to create a peer-to-peer transactions architecture that is smart, safe, and efficient. The health caresystem could drastically change thanks to blockchain, a horizontal platform that has already revolutionized numerous industries. This article's objective is to critically evaluate 50 articles on blockchain-based health systems that were published between 2015 and 2020. Thirty-six of these were journal articles, seven were from conferences, four were from different symposiums, three were from seminars, and one was a chapter from a book. This report will provide answers to three important questions. First, what are the latest technical developments in hospital blockchain developing applications? The second question is: How can this systematic analysis help us better comprehend the possibility of applying blockchain-based technology to the healthcare industry? What are the key obstacles to implementing blockchain as a solution in the healthcare industry, third? Many of the blockchain systems described in this article's descriptive use privately held blockchain and Ethereum platforms, according to statistical data on the tactics of these 50 articles. We also discuss potential future developments in blockchain use, such as alternate block chainarchitecture, cloud-based services, and blockchain integration with artificial intelligence.

Md Tarique Jamal Ansari et al. [2022], Adversaries are continually looking for ways to exploit weaknesses in newly developed digital healthcare technologies. Few writers have written about long-lasting application security. As a result, there is a need for a robust security system that can protect important data in an emergency while also being sufficientlyeffective and trustworthy. It guarantees that the programme can be maintained and meet users' needs for a considerable amount of time. In the context of the Digital India mission, this study proposes the fuzzy TOPSIS-based method to assess the psychological impact on lasting security. Additionally, this paper offers brand-new DURASec blueprints for the creation of reliable healthcare applications. Hospital, drugstores, pharmacies, physicians, the pharma business, as well as medical device manufacturers, should be ready to recognise and reduce cyber threats in order to preserve sensitive patient information, even when the benefits of such technology may outweigh the risks.

III. Security and Privacy Challenges

Security Challenges

Wrong access control: The services offered by an IoT device should be restricted to the administrator and the people they confide in in their immediate surroundings. Furthermore, the hardware's security system quite often fails to implement this sufficiently. IoT devices may have enough trust in the local area networks to avoid the need for additional authentication but instead authorisation. Any additional equipment capable of connecting to the same communication network is also pretty much assured. If the device is connected to the internet, the problem isexacerbated even though anyone on the planet could potentially gain access to the characteristics and attributes it provides. The software and default configurations for devices with the same blueprint are frequently the same. Assuming that the user doesn't change them, which happens regularly, the login information for the device might be used to connect all the devices in that order. IoT devices usually have an internal and externally visible personal account or authorization level. This implies that after attaining this privilege,there is no further access control. This one degree of security does not protect against severalvulnerabilities.

Excessively large attack surface: Every every system interaction presents a new set of opportunities for an intrusive party to find and exploit flaws. The more services a device offers via the Internet, the more frequently it may be endangered. The word for this is threat landscape. Lowering the attack vector is simply one of the initial steps in the process of trying to secure a system. On open ports, a device may have tasks scheduled that aren't necessarily required for proper operation. An invasion against such an unnecessary service might be easily averted by not disclosing the service. Solutions like Telnet, SSH, or an error handling feature may be vital during development even though they are rarely needed in production.

Absence of powerful encryption: A "Man-in-the-Middle" hacker can access only those data getting communicated with a remote computer or provides the correct whenever a device interacts in simple text.

Anyone with access to the network path between a device and its destination could monitor the network traffic and potentially obtain sensitive data, such as login credentials. Even if data isencrypted,

Software security flaws: Recognizing that software has security weaknesses is the first step in securing IoT devices. Due to software bugs, it would be possible to give the machine skills that the designers had not intended. In some cases, this can result in the attacker attempting to run their own script on the system in order to get sensitive information or carry out an attack on someone else. When creating an application, security issues cannot be completely avoided. All software bugs are like this. However, there are techniques to avoid common security issues or reduce the risk that they will occur. This entails following suggested practices to stop application defects, such as consistently validating input**.**

Outdated software: To ever be shielded from a security vulnerabilities, it must first be unearthed and patched., it is critical to disseminate the improved version of the programme. This means that IoT devices must ship with up-to-date software that is devoid of known vulnerabilities andupdate features to correct any security flaws found after the system is put into place.

Privacy Challenges

IoT poses a lot of threats to information privacy. The following is an overview of the various privacy challenges that companies and people may face.

Collection, use and disclosure of IoT data: Sensors such as microphones, motion sensors, and thermometers are commonly used in IoT devices to collect data. These sensors frequently generate incredibly thorough and precise data. This degree of precision makes it simple to develop more functionalities using computer vision presumptions and other efficient knowledge management, which can yield results that would have been impossible to obtain with coarser data. Besides which, sensor fusion, a methodology that combines multiple different sensors or mobile devices found close to each other, enables more systematic and accurate inferences than would otherwise be possible.

De-identification of IoT data: Humongous IoT landscapes, such as ubiquitous computing, generate massive amounts of data that can be employed for a wide range of purposes, which would include procedures areset and research. Making this data digitally available to the entire public is a popular technique for maximising its usefulness. Furthermore, datasets containing critical classified information should never be made public. Allowing individuals to remain pseudonymous by never analyzing information that has the potential to identify them is a relatively simple method of ensuring that confidential communications does not end up in a dataset. Instead ofusing images or videos to count people on bikes, a smart city could use IoT embedded sensors that detect movement to count them. The process of removing personal informationis known as de-identification. share information and knowledge from a dataset Furthermore, because of its highly granular nature, IoT data is usually difficult to de-identify. Longitudinal data, even when pooled, is notoriously difficult to contra.

Interoperability: In recent years, the rapid development of the Internet of Things (IoT) has resulted in the development of a variety of devices, infrastructure facilities for Software And Applications (APIs), file formats, recommendations, and frameworks. An API allows a person to query ortell a computer in order to acquire a result or for a technology to interact with another computer. Because equipment, software, and data purchased from one seller frequently do not work with those purchased from another, major interoperability issues have arisen.When consumers' or organizations' data is maintained in seller "silos" that are incompatible with others, data mobility challenges can occur, making it difficult to transfer suppliers while preserving synchronization.

IV. CONCLUSION

The Internet of Things is predicted to fast grow, tying together more aspects of our daily lives and blurring the lines between online and physical locations. In the end, it's a tool that might be useful to everyone. Additionally, the growth of IoT would create new options for the collecting of private details and increase the total volume of data collected The purpose of this study is to present reader with a basic introduction to the Iot technology, together with the significant privacy and security. The system must then terminate the attacker's software and notify the user of a problem if it is compromised. Traditional security measures are ineffective in Internet of Things (IoT) systems because to the interdependence of the sensing devices, the resource limitations, and the architecture design. Components are not usable. Strong network security

infrastructure isrequired to stop unauthorised access to user data, safeguard their privacy, and reduce security and privacy threats. So it is essential to invest more money in initiatives utilising this and other cutting-edge technology. In today's digital environment, we require a robust IoT framework, deep learning, machine learning, and embedded devices to improve corporate operations and function. By utilising this potent cutting-edge technology to its full potential, humans can gain from the intelligent capabilities, features, and efficiency of wirelessly connected ecosystems.

References

[1] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[2] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[3] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Privacy-Preserving Federated Learning for IoT Devices with Secure Model Optimization", International Journal of Communication Networks and Information Security (IJCNIS), (2021), 13(2), 396–405.

[4] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimizing AI-Driven Security Protocols in IoT Networks Using Metaheuristic Algorithms", International Journal of Intelligent Systems and Applications in Engineering, IJISAE, 2024, 12(23s), 3339–3347.

[5] Naveen Sai Bommina, Nandipati Sai Akash, Uppu Lokesh, Dr. Hussain Syed, Dr. Syed Umar, "A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume: 11 Issue: 3.

[6] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[7] Nandipati Sai Akash, Uppu Lokesh, Naveen Sai Bommina, Hussain Syed, Syed Umar, "Swarm Intelligence-Based Hyperparameter Optimization for AI-Powered IoT Threat Detection", International Journal of Intelligent Systems and Applications in Engineering, (2024), 12(17s), 941.

[8] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[9] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[10] Habeeb, M. S., & Babu, T. R. (2024). MS-CFFS: Multistage Coarse and Fine Feature Selection for Advanced Anomaly Detection in IoT Security Networks. International Journal of Electrical and Electronics Research, 12(3), 780-790.

[11] Ahmad, Z., Khan, A. S., Aqeel, S., Julaihi, A. A., Tarmizi, S., Annuar, N., & Habeeb, M. S. (2022, May). S-ADS: spectrogram image-based anomaly detection system for IoT networks. In 2022 Applied Informatics International Conference (AiIC) (pp. 105-110). IEEE.

[12] HABEEB, M. S., & BABU, T. R. (2024). WOA-SA: OPTIMIZING NIDS WITH ENHANCED DEEP LEARNING FOR ZERO-DAY ATTACK DETECTION. Journal of Jilin University (Engineering and Technology Edition).

[13] Divya Rohatgi, Dr. Tulika Pandey, "Regression Test Selection Framework for Web Services", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020.

[14] R. Gnanakumaran, Divya Rohatgi, A K Sampath, Nidhi Nagar, D. Amuthaguka, Raj Kumar Gupta, "Robust Extreme Learning Machine based Sentiment Analysis and Classification", 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), (2023), DOI: 10.1109/ICSSIT55814.2023.10061017.

[15] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[16] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[17] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Privacy-Preserving Federated Learning for IoT Devices with Secure Model Optimization", International Journal of Communication Networks and Information Security (IJCNIS), (2021), 13(2), 396–405.