Journal of Data Science and Cyber Security, ISSN: 2584-0010, Volume 1 Issue 1 June 2023

Security Concerns and Major Challenges in IoT: A Review

Shambhu Sharan[1, *], Poonam Bansal[2] and Sharvan Kumar[3]

[1]Centre of Excellence – Artificial Intelligence, Indira Gandhi Delhi Technical University for Women, India; shambhusharan@igdtuw.ac.in

[2]Artificial Intelligence & Data Sciences, Indira Gandhi Delhi Technical University for Women, India, India; poonambansal@igdtuw.ac.in

[3]Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, India; sharvanrewri@gmail.com

***Corresponding Author:** Shambhu Sharan (shambhusharan@igdtuw.ac.in)

Abstract

The Internet of Things (IoT) is basically a wireless communication system in which different IoT gadgets referred to as smart nodes communicate with one another to transmit and receive data over some communication media. Smart buildings, congested road management, surveillance systems, managing environmental waste, emergency services, transport management, ecommerce, industrial control, and intelligent healthcare system etc., are few examples of IoT applications. Technologies seem to have become vital for individuals to employ in order to construct smart systems. It enabled individuals to communicate more effectively. Unfortunately, the intruders unlocked the way for assaults on IoT infrastructure in order to steal crucial user data. However, because internetwork connections are involved, it provides the opportunity for intruders to infiltrate IoT networks and make use of the critical and sensitive user information. Because the Internet of Things provides a possible foundation for incorporating any sort of networked and sophisticated system, it may meet security flaws rooted in the different systems present inside the interconnected platform. This paper attempts to analyse the security problems of one or more systems accountable for IoT connectivity, as well as their influence on the overall IoT ecosystem.

Keywords

IoT Security Attacks, Internet of Things, IoT Security, IoT Systems, IoT, Network security.

1. Introduction

The Internet has a substantial economic and social influence by providing remarkable connectivity and communication facilities [1], [2]. It has become increasingly pervasive since the introduction of cheap wireless connections. Huge numbers of individuals are now linked to the Internet through portable and handheld personal devices thanks to developing technology. The projected huge step beyond this level is that networked devices share information with interconnected nodes.

The IoT is a recent fad and growing concept in the globe today. It is essentially a collection of hardware objects or physical gadgets that link over the internet to interact and communicate with one another and with the human beings [3], allowing the user to supervise or manage them from anywhere, as illustrated in Fig. 1 [4]. As technology spreads, connecting to the internet has become a critical prerequisite for society, hospitals, universities, and homes, to name a few. According to statistical statistics, the number of IoT linked devices have reached around 13.1 billion in 2022, up from 11.3, 9.7, and 8.6 billion in the preceding three years [5]. Furthermore, it is expected to reach about 29.4 billion by 2030. IoT is becoming the technology of the future due to its rapid expansion. The IoT system is often integrated with detectors and sensors, which gather various data and send it through the network with the objective of analyzing, regulating, or making choices [6]. The majority of such data are gathered instantaneously in order to make the best judgment regarding the device status. Furthermore, the unprocessed information captured from the devices through the internet must be translated to readable form so that the user may learn about the gadgets.

IoT, just like every other state of the art, is vulnerable to malevolent individuals including hacktivists

[7]. As the Internet of Things expands, different privacy and security challenges emerge, while the conventional privacy and security vulnerabilities worsen. Its main fundamental causes are the objects' vast magnitude and heterogeneous nature. The vast & complicated topology of IoT renders it simple to identify vulnerabilities through which cyber attackers might attack and manipulate IoT networks. Cybercriminals might enter inside IoT networks, damage them, prevent them from operating, and abuse the information, among other things. Because IoT systems have always been critical, they should definitely be protected, i.e., all security gaps must be filled. Users would prefer to use IoT networks that provide greatest degree of confidentiality and protection. It is quite impossible to utilise an IoT application with comprehensive functionalities and confidence without some kind of protected infrastructure [8]. IoT networks communicate personal data, making user safety and confidentiality a top issue. Many types of security vulnerabilities exist in IoT platforms. Few of these privacy and security related vulnerabilities can be triggered by cyber-attacks on various architectural layers of IoT, whereas others may be induced by misusing the characteristics of network communication to penetrate into and hack the system modules in order to harm them [9], [10]. Our work delves into confidentiality & safety measures, as well as the problems of IoT.

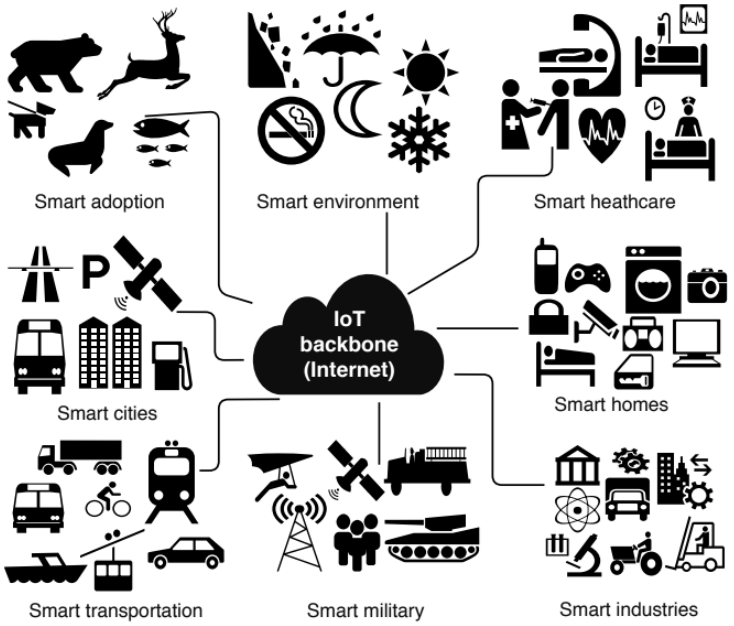

Fig. 1. A broad overview of the Internet of Things [4].

2. Literature Review

There have been several researched studies that conducted surveys on IoT security and the issues that IoT systems and gadgets in the system face. To discover an efficient approach to IoT security difficulties, we must first thoroughly comprehend the privacy and security concerns of IoT. This section of the present paper outlines few of existing research activities and gives a summary of the literature on such concerns.

Roman et al. provided a vulnerability assessment of IoT based on centralized and distributed architectures [11]. The authors investigated numerous attack scenarios in both IoT architectures and found that a compact and robust protection solution against IoT threats would always be required.

Sarrab et al. examine IoT privacy problems in the domain of healthcare and present a comprehensive paradigm of IoT dataflow including security risks [12]. Furthermore, the authors explore confidentiality within IoT dataflow, particularly in healthcare system, and provide confidentiality measures needs to be

maintained in every stage. Their findings revealed that confidentiality in IoT occur at several phases of the dataflow, with distinct sorts of security issues including countermeasure strategies at every level of IoT data.

Atlam et al. examine IoT safety, confidentiality, security, and moral standards [13]. The authors began by offering a comprehensive introduction to IoT system, including its design and key characteristics, before delving into IoT security issues, needs, and best practises for protecting the nodes in the IoT infrastructure. They additionally covered IoT confidentiality by emphasising several potential risks and ways to protect IoT equipment security and confidentiality. They particularly covered IoT wellbeing, morality, importance for ethical prototype, and obstacles observed. Finally, smart cities are used as a research example to analyse potential safety issues and offered remedies for maintaining a high degree of security in a smart city.

Kaur et al. investigate possible effect of big data issues, research activities aimed at IoT data evaluation, including different methodologies related to its assessment [14]. It highlights some of the concerns and challenges that big data presents, one of which is the collection of insight from IoT data. The authors analysed several study subjects, varied possibilities provided by data assessment with in IoT ecosystem, obstacles and technologies utilised for BDA, and the data privacy component of BDA. Because each Big Data framework seems to have its own unique methodology, the authors proposed using platforms to study big data in phases. All sorts of equipment interact with one another in a variety of manners.

Lee et al. expand current confidentiality and security vulnerability concepts to show the value of architectural protection and user security risk safeguards in home IoT systems [15]. The authors carried out an experimental study on 265 specimens using a fractional least squares structural equation modelling approach to evaluate their suggested methodological approach. Gender, expertise, and dwelling style were used to compare variations in susceptibility characteristics, as well as concerns about privacy and reluctance to household IoT services. According to the findings, user vulnerability most of the time has the greatest influence on household IoT privacy issues and intolerance to household IoT settings. Furthermore, the authors discovered that personal characteristics fluctuate across vulnerabilities, confidentiality issues, and household IoT resilience.

Idrissi et al. examine the current status of IoT security risks and loopholes by classifying certain previously known vulnerability concerns using the Cisco IoT baseline architectures [16]. The authors then conduct a study of existing studies in the field of IoT security, focusing on Intrusion Detection Systems (IDS) built on deep learning, which are developing as new approaches in a variety of domains, notably cybersecurity. The insights might form the foundation for subsequent scientific pathways.

According to Yao et al., digital gadgets security and privacy are critical to the linked technologies [17]. To simplify the difficult privacy protection considerations, a physical object's life cycle is separated as 3 different stages i.e., pre-working, post-working & in-working, by the authors. Upon that premise, a physical object-based privacy architecture for the IoT is proposed. The authors thoroughly examine the privacy and security needs, as well as associated protection technologies, for physical objects at various phases of development. The possible privacy and security problems that IoT items might encounter within ubiquitous computing environment are described in light of the advancement of IoT technology. Simultaneously, different alternative approaches to coping with these issues are suggested by the authors.

In the context of IoT, Parashar et al. addressed various attack scenarios [18]. The authors concentrated on the possibility of hacking a system or disabling services in the middle of a transmission. They addressed how hackers might remotely disrupt the two differently paired medical device and modify their settings, causing medicine delivery to halt. The authors also explained how attackers may infiltrate a car's underlying communications system without even having to touch the vehicle, gaining access to everything within and even controlling the engine and breaking mechanisms.

3. DISCUSSION

3.1 Recommended Strategy to IoT Security

It may look difficult at first to protect IoT, although it is possible via early preparatory work, because security considerations in the early stages might address significant IoT security challenges. Protection is often applied at the organisational level after studying and assessing the entire risk associated with the functioning of secure rules and standards. Any firm may tackle IoT security challenges to greatest extent feasible by examining data security threats and the policies necessary to safeguard data that are relevant to the devices they actually function on, as well as device security. This technique simplifies the development of any IoT architecture while also providing the added benefit of applying and integrating existing established security standards into the present world of technology. As a result, this technique necessitates a detailed grasp of the distributed modules, respective limitations, and their implementing capabilities. Because these IoT devices possess its own respective operating systems, each IoT device is built on a network stack that is primarily made up of wireless networking architecture and technology. The operating system within IoT gadgets might be shut down to protect the devices against vulnerabilities caused by cyberattacks and threats, which would necessitate constant inspection of operating system services or maintaining adequate infrastructural protection depending on viable solutions. The vulnerabilities caused by insecurity put the operating system in jeopardy, although security prevention may be done via regular attention and coordinated maintenance programmes, or by installing some kind of shield like firewall. However, adopting this technique to provide protection will be restricted to a network with very few gadgets; alternatively, in the event of several gadgets, it would be necessary to automate and synchronise, which may aid the network in minimizing human mistakes.
While IoT systems communicate wirelessly by means of wireless ethernet adaptor or Bluetooth, such technology solutions can employ crucial software upgrades including modifications to fix earlier flaws or even uses more advanced framework to swiftly resolve security risks. The architecture is reliant on the cryptography mechanisms used among communicating or talking nodes to assure peer-to-peer connectivity utilising distinctive key pairs. Additional level of protection comprises every device that attempts to access the network, which is dependent on the organisational policies for way through the system process execution. The third critical layer is responsible for managing and splitting communication routes, which is performed by categorising objects network-wide. With the exception of regulating numerous different network devices, the firewalls (including IP-based and Bluetooth based) might be excellent countermeasures against cyber-attacks. The paper also addresses an appropriate IoT architecture, as illustrated in Fig. 2, comprising of 3 layers that might act as a secure standard architecture for IoT devices [19].

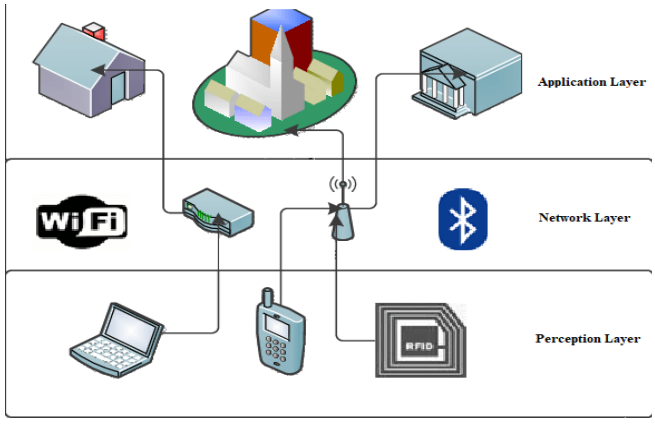

Fig. 2. IoT Architecture [19].

3.2 An IoT Security Architecture

The IoT possesses tremendous opportunities, mainly with primary objective of transforming the manner in which individuals execute various tasks and reforming individual's life patterns in the contemporary age. As a result, the concept of IoT varies depending on the sort of application we aim to design. The technological IoT architecture is made up of four core ingredients i.e., Devices/Gadgets, Sensors/Detectors, Gateways and Clouds [20]. However, there are numerous types of issues linked with the IoT infrastructure of gadgets and their administration. One of the main goals of this analysis is on security concerns and difficulties from an IoT viewpoint that is based on network security problems and layer protection. To address the key challenges and possibly future alternatives that render the systems secure against cyberattacks, overall architecture of the IoT platform with reference to three levels (i.e., perception layer, network layer, and application layer) must be investigated. Security and privacy problems are important considerations in IoT technology. The needs for privacy and security fulfilment play a key role, with the requirements include access control via distributed systems, encryption and authentication of information, confidentiality and trustworthiness among objects and people, and the strengthening of safeguards and confidentiality legislation. Fig. 3 depicts the IoT security problems [21]. The primary needs for IoT security are to guarantee that data is always available to authorised users. IoT has several uses with varying economic impacts spanning from home to business, and it is rapidly expanding to enable everyday actions to become a part of the global system. As the Internet of Things expands, so do the security concerns, and techniques to securing systems and sensors progress toward increasing autonomy in responding to assaults and identifying risks, depending on a systemic cognitive strategy. As a result, effective cybersecurity approaches based on constrained resources, applications, and highly secure standards, such as authenticating procedures, credentials and identity handling, are necessary for embedded systems. Security is critical in the development of IoT applications. Furthermore, IoT applications collect massive amounts of information from a wide range of detectors. As a result, this data must be safeguarded by information management technologies such as cryptography, as the majority of this data is confidential and sensitive, and the gathering and use of private data is one kind of privacy IoT problem in and of itself.

Fig. 3. IoT Security Challenges [21].

3.3 Security Concerns at the Perception Layer

This layer is considered as lowest layer in the traditional IoT ecosystem. The primary purpose of the perception layer is acquiring meaningful and appropriate data from items or the surroundings, including such Wireless Sensor Network (WSN), embedded system, detectors type realworld entities, moisture, and heat, among others. Radio Frequency Identification (RFID), WSN, and other forms of detection

and monitoring methods are the primary underpinning technologies used in this layer. This layer prioritises the following attack types:

- Node Capture: The network gateway nodes are more vulnerable to being compromised, which might also result in critical data leakage that jeopardises the security of whole network.
- Malicious Node: In this form of security problem, the adversaries install a malevolent module to the current system via which they may distribute harmful data across the network and corrupt the entire system.
- Denial of Service (DoS): Attackers take advantage of the node's limited processing power to disrupt the network.
- Distributed Denial of Service (DDoS) Attack: DDoS assaults have been the common & most easiest to carry out across systems, whereby they result in service outages and overall network depletion.
- Replay Attack: The adversary uses the replay attack to breach the authenticating mechanism and network trust by replaying prior communications to the target node.
- Routing attacks: An intermediary malicious node modifies the routing path and makes the system busy throughout the data gathering and transmission procedure.

3.4 Security Concerns at the Network Layer

The network layer grants the previous layer i.e., perception layer, global accessibility, by way of receiving data from it and transmitting the same to a specified data framework via the application layer. Man-in-the-middle attacks, Network intrusion, and eavesdropping are the most common vulnerabilities at this layer. These possible risks concern relates to trustworthiness, secrecy, and easy accessibility.

- Data Revelation: By exploiting social engineering processes, the adversary might well be capable of obtaining crucial information through the system. Despite the fact that the IoT network has a large number of gadgets or nodes with a large volume of data, it is simple to obtain the data out from nodes by applying particular information retrieval procedures.
- Heterogeneity: As a result, the framework is susceptible. The engagement and use of diverse techniques, networking alignment, as well as security policy compliance are the key reasons for the system's heterogeneity.
- Issues of Scalability: IoT comprises a significant variety of connected devices, some of which are quite large, and these could leave or access the system several times, adding to the issues of network congestion, a lack of identification and authorisation, a shared environment, and so on. It also uses up a lot of resources.

3.5 Security Concerns at the Application Layer

This layer necessitates varying levels of security based on needs of the application, making application security procedures convoluted and difficult. This layer addresses privacy and security concerns as well.

- Mutual authentication and node identification: Varying forms of authorized access are necessary for every application for determining appropriate nodes to handle authentication, and this is calculated on the basis of users authorised by a given application. This vulnerabilities at this layer. These possible risks concern relates to trustworthiness, secrecy, and easy accessibility.
- Data Revelation: By exploiting social engineering processes, the adversary might well be capable of obtaining crucial information through the system. Despite the fact that the IoT network has a large number of gadgets or nodes with a large volume of data, it is simple to obtain the data out from nodes by applying particular information retrieval procedures.
- Heterogeneity: As a result, the framework is susceptible. The engagement and use of diverse techniques, networking alignment, as well as security policy compliance are the key reasons for the system's heterogeneity.
- Issues of Scalability: IoT comprises a significant variety of connected devices, some of which are quite large, and these could leave or access the system several times, adding to the issues of

network congestion, a lack of identification and authorisation, a shared environment, and so on. It also uses up a lot of resources.

4. Conclusion

As the number of IoT-connected gadgets grow recently and will further continue to grow in the coming subsequent years, so will the cyberattacks to information safety and confidentiality linked with these gadgets. As a result, there is an urgent need to establish security across all systems used to interconnect the smart devices within IoT platform. To summarise, it is necessary to be cautious and select an IoT gadget depending on the gadget's capacity to provide protection against security breaches. To create a safe IoT framework, evaluating the limitations of IoT devices, analysing network architecture, vulnerability categories, and organisational risk potential is very much crucial. It is very much necessary to develop a solid network infrastructure to accommodate the IoT modules, even while vulnerabilities may be addressed efficiently and conveniently in the network.

In the future, we hope to create a real-world implementation of a robust and highly secured IoT framework, so as to demonstrate how to solve IoT security concerns using simulations of networking models, and highlight the potential necessity of allowing authorised access to crucial data.

References

[1]. S. Villamil, C. Hernández, and G. Tarazona, “An overview of internet of things,” Telkomnika (Telecommunication Comput. Electron. Control., 2020, doi: 10.12928/TELKOMNIKA.v18i5.15911.

[2]. E. Zhuravskaya, M. Petrova, and R. Enikolopov, “Political effects of the internet and social media,” Annual Review of Economics. 2020. doi: 10.1146/annurev-economics-081919-050239.

[3]. W. Choi, J. Kim, S. E. Lee, and E. Park, “Smart home and internet of things: A bibliometic study,” J. Clean. Prod., 2021, doi: 10.1016/j.jclepro.2021.126908.

[4]. K. Lounis and M. Zulkernine, “Attacks and Defenses in Short-Range Wireless Technologies for IoT,” IEEE Access, 2020, doi: 10.1109/ACCESS.2020.2993553.

[5]. L. S. Vailshery, “Number of IoT connected devices worldwide 2019-2030,” 2022. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed Jul. 15, 2022).

[6]. N. M. Kumar and P. K. Mallick, “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers,” 2018. doi: 10.1016/j.procs.2018.05.170.

[7]. P. Ferrara, A. K. Mandal, A. Cortesi, and F. Spoto, “Static analysis for discovering IoT vulnerabilities,” Int. J. Softw. Tools Technol. Transf., 2021, doi: 10.1007/s10009-020-00592-x.

[8]. C. C. Uchenna, N. Jamil, R. Ismail, L. K. Yan, and M. A. Mohamed, “Malware threat analysis techniques and approaches for iot applications: A review,” Bull. Electr. Eng. Informatics, 2021, doi: 10.11591/eei.v10i3.2423.

[9]. M. Alanazi and A. Aljuhani, “Anomaly Detection for Internet of Things Cyberattacks,” Comput. Mater. Contin., 2022, doi: 10.32604/cmc.2022.024496.

[10]. V. Dutta, M. Choraś, M. Pawlicki, and R. Kozik, “Detection of cyberattacks traces in IOT data,” J. Univers. Comput. Sci., 2020, doi: 10.3897/jucs.2020.075.

[11]. R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” Comput. Networks, 2013, doi: 10.1016/j.comnet.2012.12.018.

[12]. M. Sarrab and F. Alshohoumi, “Privacy concerns in IoT a deeper insight into privacy concerns in IoT based healthcare,” International Journal of Computing and Digital Systems. 2020. doi: 10.12785/IJCDS/090306.

[13]. H. F. Atlam and G. B. Wills, “IoT Security, Privacy, Safety and Ethics,” in Internet of Things, 2020. doi: 10.1007/978-3-030-18732-3_8.

[14]. M. Kaur and A. M. Aslam, “Big Data Analytics on IOT Challenges, Open Research Issues and Tools,” Int. J. Sci. Res. Comput. Sci. Eng., 2018, doi: 10.26438/ijsrcse/v6i3.8185.

[15]. H. Lee, “Home IoT resistance: Extended privacy and vulnerability perspective,” Telemat.

Informatics, 2020, doi: 10.1016/j.tele.2020.101377.

[16]. I. Idrissi, M. Azizi, and O. Moussaoui, "IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review," 2020. doi: 10.1109/ICDS50568.2020.9268713.

[17]. X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," Digital Communications and Networks. 2021. doi: 10.1016/j.dcan.2020.09.001.

[18]. A. Parashar and S. Rishishwar, "Security challanges in IoT," 2017. doi: 10.1109/AEEICB.2017.7972351.

[19]. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2016. doi: 0.1109/ICITST.2015.7412116.

[20]. SumatoSoft, "What is IoT Architecture | 4 stages of IoT Architecture," 2021. https://sumatosoft.medium.com/what-is-iot-architecture-4-stages-of-iot-architecture-e2c19a1616 (accessed Aug. 01, 2022).

[21]. M. A. Al Ghamdi, S. H. Almotiri, M. Alruily, M. M. Iqbal, U. Khadam, and M. Ramzan, "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions," WCMC, vol. 2020, pp. 1–15, Feb. 2020, doi: 10.1155/2020/7105625

[22]. Pabreja, K. Sharma, T. Jatain, A. Bhaskar, S. (2023) Literature Review: A Comparative Study of Software Defect Prediction Techniques. Proceedings of 3rd International Conference on Artificial Intelligence: Advances and Applications: ICAIAA 2022, 13-29.

[23]. Sharma, T. Jatain, A. Pabreja, K. Bhaskar, S. (2023) Ensemble Machine Learning Paradigms in Software Defect Prediction. Procedia Computer Science, 218, 199-209.

[24]. Jatain, A. Tripathi, K. Bhaskar, S. (2022) Deep Learning-Based Object Recognition and Detection Model. Deep Learning in Visual Computing and Signal Processing, 123-143.

[25]. Jajula, S. K. Tripathi, K. Bhaskar, S. (2022) Review of Detection of Packets Inspection and Attacks in Network Security. Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, 1, 597-604.

[26]. Joy,T.D. Prangyanidhi, S. Jatain, A. Bhaskar, S. (2022) Artificial Intelligence Aided Neurodevelopmental Disorders Diagnosis: Techniques Revisited. Machine Intelligence and Smart Systems: Proceedings of MISS 2021, 1-8.

[27]. Singh, R. Shrivastava, S. Jatain, A. Bhaskar, S. (2022) Deepfake Images, Videos Generation, and Detection Techniques Using Deep Learning. Machine Intelligence and Smart Systems: Proceedings of MISS 2021, 501-514.

[28]. Dalal, S., Seth, B., Radulescu, M., Secara, C., & Tolea, C. (2022). Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model. Mathematics, 10(24), 4679.

[29]. Dalal, S., Onyema, E. M., & Malik, A. (2022). Hybrid XGBoost model with hyperparameter tuning for prediction of liver disease with better accuracy. World Journal of Gastroenterology, 28(46), 6551-6563.

[30]. Zaki, J., Nayyar, A., Dalal, S., & Ali, Z. H. (2022). House price prediction using hedonic pricing model and machine learning techniques. Concurrency and Computation: Practice and Experience, 34(27), e7342.