International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 495-500

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/6fzpzd03
Research paper

IOMT Security and Anomaly Detection in Medical Images Using AI

Dr. Nidhi Mishra *, Ashu Nayak

Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India
**Corresponding author E-mail: ku.nidhimishra@kalingauniversity.ac.in*

Received: June 10, 2025, Accepted: June 17, 2025, Published: November 1, 2025

Abstract

The extensive use of information and communication technology (ICT) has transformed every aspect of life as the world moves closer to digitalization. There is no denying that ICT has changed how people communicate, live, work, and study. The Internet of Things, or things, is a powerful combination of critical ICT technologies, with integrated hardware, software, and other technologies for connecting and sharing data with other systems and devices over the Internet. An Internet of Things (IoT) device is any electronic device that can be used in a wide range of social contexts, including connected industries, transportation, healthcare, smart supply chains, smart farms, smart cities, smart grids, and many more. This includes wearable technology and hardware. The Internet of Medical Things (IoMT) is a real-world application of the Internet of Things (IoT) in the healthcare sector, enabling patients to receive better healthcare and enjoy a higher quality of life. It provides seniors and patients with real-time healthcare services, support, and caregiving using Internet-enabled smart devices. The current coronavirus disease (COVID-19) has increased the demand for remote patient care due to a paucity of resources and healthcare facilities, in contrast to the enormous global demand for these services and facilities. Therefore, COVID-19 has played a significant role in the shift of the present healthcare system towards remote care. Even with advancements in the healthcare sector and the apparent benefits of integrating it with IoT, moving all forms of communication online is a logical next step. It opens the door for potential security lapses in the ongoing IoMT communication, providing adversaries with unauthorized access to vital health data that could be misused for malicious intent.

Keywords: *Information and Communication Technology; Internet of Things; Internet of Medical Things; Security; Authentication; Access Control; Key Agreement; Simulation.*

1. Introduction

In the current state of wireless communication, there has been a notable boom in the Internet of Things (IoT). The Internet of Things (IoT) can be defined as things, or items, connected to the Internet that provide and access real-time data [16]. An Internet of Things (IoT) device is any electronic device, from wearables to hardware, with a wide range of applications in transportation, healthcare, and smart homes [1]. The information is persistently sensed by smart appliances found in smart homes such as smart TVs, smart devices in patients' bodies such as brain neuro stimulators, smart cars and smart traffic management appliances, smart appliances in industries to monitor the industries as well as environment, etc., and then sent to dedicated servers where necessary processing and analysis is performed for monitoring and control purposes [17]. Compared to existing Internet services, the Internet of Things offers several advantages. To oblige every single object that is presently or may someday be a part of the Internet of Things network is the aim of attaching everything [2]. The idea of tying all of that together at some point is fascinating [18]. Currently, the Internet of Things connects billions of devices for usage in a variety of vertical applications, including healthcare. The Internet of Things has significant potential for the healthcare industry. A specific subset of the Internet of Things, known as the Internet of Medical Things (IoMT), comprises individually identifiable medical equipment that is networked and capable of communicating with one another. It enables remote/automated resource management, real-time information exchange, and asset localization [3]. It ensures both patient safety and excellent care within the allotted timeframe [19]. The utilization of the IoMT environment has made it possible to access patient healthcare data and equipment continuously, as well as to manage medical facilities effectively and efficiently. Remote patient monitoring, hospital operations management, remote surgery, and other critical applications are among the numerous uses of IoMT [20].

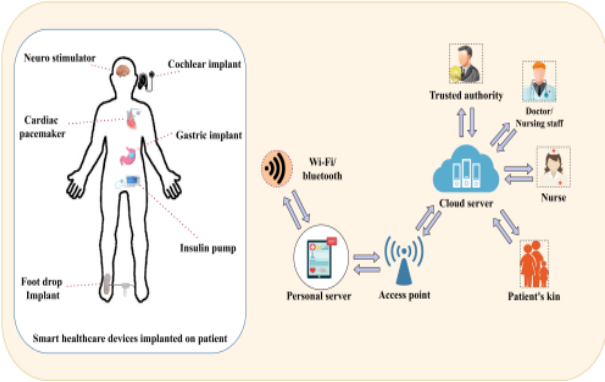

Fig. 1: IoMT Communication Environment.

By 2020, the IoMT market is expected to reach $ 136.8 billion. Finally, the connection between sensors and medical equipment streamlines clinical work process management and encourages overall improvements to patient care from the inside out [21].
The paper's next section is structured as follows: Section 1 presents a view of IoT/IoMT and its various scenarios. Then we discuss various security requirements and types of potential attacks in the IoMT network in Section 2. Section 3 proposed a new "privacy-preserving access control and key management mechanism" to safeguard communication done by the IoT-based e-health system (SPCS-IoTEH). Section 4 describes the experiment that was conducted utilizing a novel technique. Section 5 presents the work's conclusion. It also outlines the future scope of the investigation.

2. Problem Statement and Objectives

These days, Internet-enabled smart IoT devices have become an essential part of our daily lives since they complement and facilitate our workouts. They must secure their communication because the Internet of Things (IoT) is becoming more and more important. This is especially true for the healthcare industry, where all communication occurs over an insecure open channel that is vulnerable to attacks [22]. Additionally, it made it possible for attackers or intruders to get unauthorized access to the ongoing communications between the IoMT data exchange network's entities and to add, alter, or remove malicious data from the network [5]. Additionally, attackers can get unauthorized access to smart IoMT devices and remotely operate them. This may put people at risk. For example, if a patient's smart pacemaker is damaged, shock may result in the patient's death [23]. IoMT data exchange within the network needs to be protected because of the problems that result from assaults. Sensitive patient-centric data and smart healthcare equipment must be authenticated, confidential, available, and intact, among other security and privacy needs. Non-repudiation, freshness, forward and backward secrecy, among many other things, are additional security criteria [6]. These security methods are resistant to several possible attacks because of their many features. Attackers create new, more efficient techniques to gain unauthorized access to the IoMT data exchange network and conduct a variety of active and passive attacks as technology develops [7]. Therefore, for the purpose of sending sensitive healthcare data between smart healthcare devices and other network entities, we require an extremely safe, impenetrable communication environment [24]. Furthermore, it is crucial to protect these smart medical gadgets from being stolen or misused by unauthorized individuals who could use them for nefarious purposes. Although several security methods have been developed in the past, there is always room for improvement to create a system that is more secure and resistant to any threats.
Connections between different entities in the communication within the IoMT network environment, such as smart medical devices, servers, and users, need to be secure and always available due to the extremely sensitive nature of the information being handled in this context. Furthermore, data availability, confidentiality, and integrity are important for medical information to be exchanged across the hospital network. [8].

2.1. Comparison with the existing IoMT security frameworks

The SPCS-IoTEH model represents considerable improvements over the current IoMT security systems, including the one by He-Zeadally and Jang, especially when it comes to communication overhead. Although He-Zeadally uses 3232 bits and Jang uses 5920 bits to achieve secure communication, the SPCS-IoTEH framework uses only 1792 bits, improving both efficiency and scalability. These communication overhead savings are critical in real-time applications in IoMT, where low latency is a must. Moreover, the AI-centered anomaly-detection in SPCS-IoTEH will provide the system with a stronger defense against threats such as replay attacks and impersonation to strengthen security gaps in traditional models that do not consider AI implementation.

2.2. Recent research on IoMT security

Recent research has shown that there is an increasing demand for AI-based security in IoMT networks. All these studies highlight the benefits of incorporating machine learning models to identify anomalous behaviors and protect IoMT devices, which also justifies the suitability and usefulness of the framework of SPCS-IoTEH in the contemporary healthcare setting.

3. Proposed Framework

Healthcare systems receive and handle private, frequently vital medical data, and then use that data to make necessary decisions. Occasionally, there's a chance that IoMT devices contain security vulnerabilities [25]. As a result, cybercriminals might focus on these IoMT devices' weaknesses. Attackers may be able to access healthcare systems and equipment, as well as obtain sensitive personal and medical data without authorization. Cyberattacks on healthcare systems and devices have the potential to seriously hurt linked patients as well as cause any form of damage.

The implementation of IoMT has become a crucial necessity for the healthcare system because it is used in many applications and sub-domains. It's crucial to talk about the possibility that it has various security and privacy-related problems, though. Numerous attacks are feasible, including but not limited to some other attack. Presenting security measures is therefore essential to stop attacks and the related IoMT data. Many of these strategies have been presented recently; however, as was previously said, most of them raise security problems because they are vulnerable to assaults. [9].

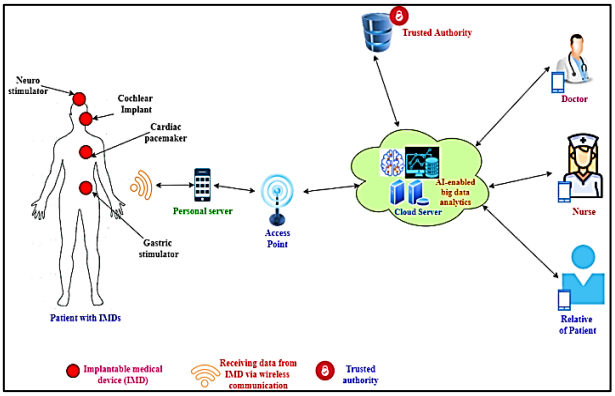

Fig. 2: Overall Architecture.

3.1. System model

In Fig. 2, the network model is displayed. It shows a patient who has had many medical implants. Medical or monitoring devices include things like cardiac pacemakers, gastrostimulators, cochlear implants, and neurostimulators. Data from the implanted medical device (IMD) is gathered by a personal server situated near the patient, using WiFi, Bluetooth, or other wireless communication technology. The acquired data is transmitted to subsequent processing or analysis. Some users, such as doctors, nurses, and patients' families, are eager to obtain patient data. [10].

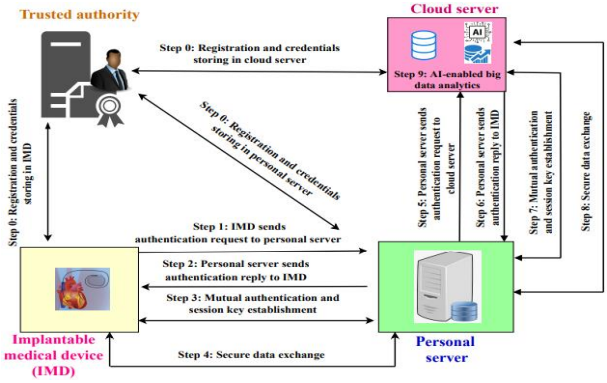

Fig. 3: Process Flow Diagram for AI-Envisioned Communication Scheme.

A trusted authority has registered several network entities. After completing the login process, users can access patient data from cloud servers. It is believed that the cloud servers are resource-rich nodes. Every communication involves the exchange of encrypted data using a session key, which is generated and transferred following the authentication procedure, to safeguard the connection between the parties. This system makes use of insignificant cryptographic methods like hash and XOR operations because the majority of IMDs have limited processing and calculating capabilities. The recommended method can be used to securely and anonymously communicate patient health-related data [11]. Furthermore, the proposed approach leverages negligible cryptography approaches to provide secure communication between devices, even with constrained resources. Furthermore, cloud servers with legal status employ AI-enabled big data analytics techniques to predict health problems in patients, like diabetic shock and heart attacks. Therefore, the suggested conspiracy is quite advantageous in terms of medical care, i.e., excellent medical supervision, treatment, and prognosis of sickness.

The strategy that is being offered is designed using the Dolev-Yao (DY) threat model [35]. Untrusted communication entities include users, personal servers, and IMDs, according to the DY model. These things exchange messages through ambiguous channels. This gives the adversary (A) the ability to modify, truncate, or change shared data. Moreover, we used the CK-adversary model (also known as Canetti and Krawczyk's adversary model) during the creation of the mechanism that was presented. It is employed to supply an authentication and key agreement scheme and is known as the current de facto standard model [12]. The deduced information can be used for nefarious purposes, such as guessing the secret credentials (password), session key computation, replay attack, device impersonation attack, and man-in-the-middle attack. Moreover, trusted authority T A is anticipated to be a fully trusted entity of the network and not be susceptible to arbitration.

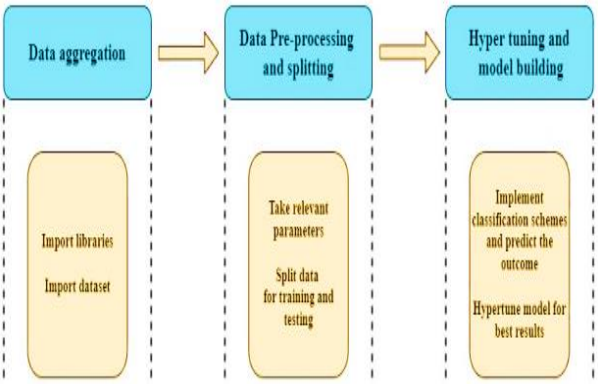

Fig. 4: AI-Based Big Data Analytics Phase.

3.2. AI-enabled big data analytics

The proposed method is covered in this article. The steps are listed and shown in Fig. as follows: registration phase, authentication and key establishment phase, dynamic device addition phase, and AI-based big data analytics phase. 3. Big data refers to extremely large amounts of diverse data. This heterogeneous data is subjected to artificial intelligence (AI) techniques in big data analytics, which is made possible by AI. These approaches make use of machine learning algorithms to sort through vast amounts of data, locate useful information, and forecast patterns for the future [13]. Because machine learning techniques can access vast amounts of diverse data, they are able to learn and forecast with great accuracy. According to this method, the AI module can learn and improve its example acknowledgment skills the more data it has access to, which increases the overall accuracy of the framework. Artificial intelligence (AI)-based big data analytics are needed to predict important outcomes from the collected data, such as the likelihood of having a heart attack [14–15]. Moreover, this procedure is run on the validated cloud server. (e.g., CSN). In this way, CSn carries out the procedure.

- CSn uses the first data aggregation technique to gather the data needed for the remaining steps of the procedure.
- The data is then separated into test and training sets so that the AI module can forecast and learn from them.
- In addition, CSn carries out more procedures.
- Following the application of these stages, the result (predictions) is observed for decision-making and other suitable actions.

4. Experimental Results and Discussion

Here, we show the performance of the proposed framework in several test cases, its performance in terms of securing communication within IoMT networks, and anomaly detection.

Dataset Description: The training and testing dataset applied to the AI-based anomaly detection module comprises 10,000 medical images obtained via the OpenI dataset, containing both X-ray images and MRI images. This dataset was selected because it is diverse and has real-world applications in the medical profession. To test the strength of the anomaly detection system, attack scenarios were injected into the data set through simulation. Such situations involve data tampering, whereby pixel values in the medical images are altered to resemble malignant alterations, replay attacks, whereby already registered images are reused to query the system on its detection capability, and impersonation attacks, whereby fake data is replaced with genuine medical images to question the detection system. This rich data enables the AI-based system to learn and detect anomalies, and it would be applicable in detecting security breaches and assuring the integrity of IoMT data exchange within various healthcare settings.

Anomaly Detection Module With AI: The AIsided anomaly detection module is tailored to identify abnormal trends in the medical images, to ensure the safety and integrity of the IoMT data exchange. This module is based on a machine learning algorithm to evaluate the medical images and diagnose any possible danger, including unauthorized entry or data modification. The system is programmed to identify common images in the photos and to report any anomaly that can point out the occurrence of a security breach. The module is an essential part of defending IoMT networks against malicious attacks as it uses advanced machine learning capabilities to keep improving its efficacy at recognizing new and unfamiliar threats.

CK Adversary Model: It simulates threats that may occur in the IoMT network by use of the CK adversary model. It presupposes that the enemies can seek access to confidential information without appropriate permission or control the communication between devices. This model assists in analyzing the security of the system, seeking to simulate attacks like device impersonation, man-in-the-middle attacks, and the framework must be able to sustain malicious attempts to weaken its security. The CK adversary model is a critical element towards putting the proposed SPCS IoTEH framework to the test, where it would be put in a real-life situation to challenge its resilience against advanced attack methodologies. With the combination of this model, the resilience of the framework to active and passive attacks is fully tested.

The proposed AI-envisioned secure communication architecture would ensure that only authorized users and devices can share sensitive patient data within the IoMT data exchange network in a secure manner.

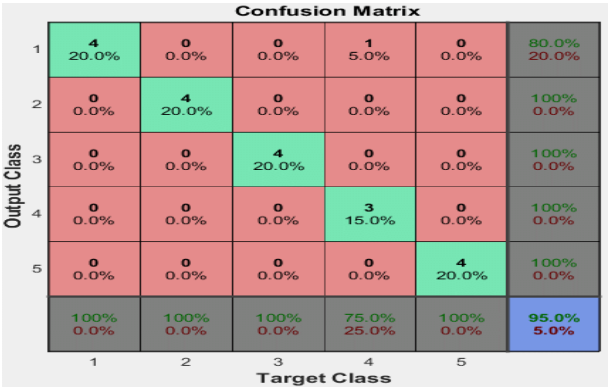

Fig. 5: Confusion Matrix for Unknown Threats.

Confusion matrix on the ability of SPCS IoTEH to distinguish known and unknown attackers (e.g., replay, impersonation) in IoMT networks. The performance of the system to detect anomalies is assessed by using the matrix to evaluate the system against different attack scenarios. Based on an informal security analysis, the scheme also shows resilience against potential attacks like physical IMD capture attacks, replay attacks, impersonation attacks, ephemeral secret leakage attacks, privileged insider attacks, and support for anonymity and untraceability properties. In addition, it provides secure session key agreement, confidentiality, integrity, and session key security under the CK adversary model. It also provides dynamic device addition and an AI-enabled big data analytics phase, which are additional security-related features and functionalities not seen in earlier schemes.

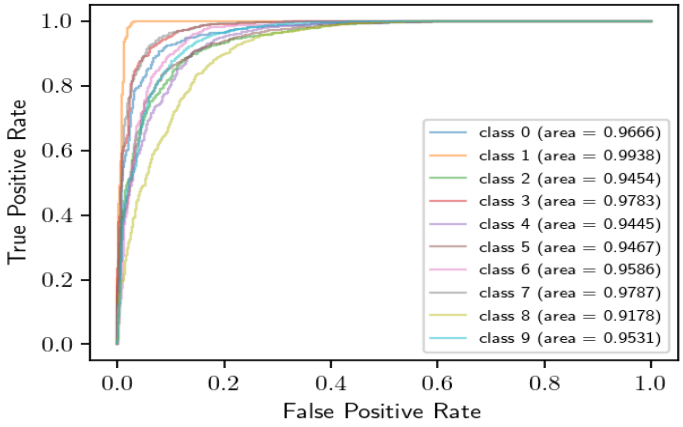

Fig. 6: ROC Curve for Known and Unknown Threats.

Receiver Operating Characteristic (ROC) curve, which shows the detection performance of SPCS IoTEH against known and unknown threats, where the true positive rate, false positive rate, and area under the curve (AUC) are used as metrics. This system is expected to require a total of 1792 bits of communication between PS and CS and 1376 bits of communication between IMD and PS. This is less than what is needed for similar systems such as He-Zeadally-3232 bits, Jang-5920 bits, Merabet-I and II-1472 bits, and so on.

5. Conclusions

The integration of medical software and hardware, such as wearable or implanted devices, that is connected to the health care information technology system through networking technologies, is known as the Internet of Medical Things (IoMT). By directly tagging patients with clinicians, needless hospitalizations are decreased, as well as the burden on the healthcare system. Additionally, it permits the safe transfer of confidential medical data via insecure networks, like as the Internet. Due to its widespread usage, several privacy and privacy concerns are bound to surface. This makes it more difficult to exchange and store private patient data securely. Medical gadgets, clinical systems, wearable technologies, and networked sensor devices are all part of the Internet of Medical Things (IoMT). It reduces overall medical costs, delivers healthcare on time, and raises the standard of service generally. While there are numerous advantages to these ubiquitous medical devices, there are also serious privacy and security challenges.

Future Directions

The way forward should be on how to scale the SPCS-IoTEH framework to support massive IoMT networks since the number of devices and data connected will increase exponentially. A major challenge is how to guarantee real-time threat detection and low communication overhead. To solve this, it is possible to utilize edge computing, where processing and analysis are done in closer proximity to the source of data, which lowers the latency as well as guarantees quicker response time. Also, the use of multi-modal information, e.g., a medical image and real-time biosignals, e.g., ECG, may enhance both precision and resilience of threat detection systems. Such integration allows monitoring the health of patients in a more comprehensive way and gives a better understanding of the possible security risks of IoMT networks.

References

[1] Ravi, V., Pham, T. D., & Alazab, M. (2023). Deep learning-based network intrusion detection system for Internet of Medical Things. *IEEE Internet of Things Magazine, 6*(2), 50–54. https://doi.org/10.1109/IOTM.001.2300021.

[2] Khan, I. A., Moustafa, N., Razzak, I., Tanveer, M., Pi, D., Pan, Y., & Ali, B. S. (2022). XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. *Future Generation Computer Systems, 127*, 181–193. https://doi.org/10.1016/j.future.2021.09.010.

[3] Edmund, A. N., Alabi, C. A., Tooki, O. O., Imoize, A. L., & Salka, T. D. (2023). Artificial intelligence-assisted Internet of Medical Things enabling medical image processing. In *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things* (pp. 309–334). CRC Press.

[4] Wazid, M., Singh, J., Das, A. K., Shetty, S., Khan, M. K., & Rodrigues, J. J. P. C. (2022). ASCP-IoMT: AI-enabled lightweight secure communication protocol for Internet of Medical Things. *IEEE Access, 10*, 57990–58004. https://doi.org/10.1109/ACCESS.2022.3179418.

[5] Muheidat, F., & Tawalbeh, L. A. (2023). AIoMT artificial intelligence (AI) and Internet of Medical Things (IoMT): Applications, challenges, and future trends. In *Computational Intelligence for Medical Internet of Things (MIoT) Applications* (pp. 33–54). Academic Press. https://doi.org/10.1016/B978-0-323-99421-7.00013-1.

[6] Ahmad, S., Khan, S., AlAjmi, M. F., Dutta, A. K., Dang, L. M., Joshi, G. P., & Moon, H. (2022). Deep learning enabled disease diagnosis for secure Internet of Medical Things. *Computers, Materials & Continua, 73*(1). https://doi.org/10.32604/cmc.2022.025760.

[7] Wagan, S. A., Koo, J., Siddiqui, I. F., Qureshi, N. M. F., Attique, M., & Shin, D. R. (2023). A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection. *Journal of King Saud University - Computer and Information Sciences, 35*(1), 131–144. https://doi.org/10.1016/j.jksuci.2022.11.007.

[8] Liu, W., Zhao, F., Shankar, A., Maple, C., Peter, J. D., Kim, B.-G., Slowik, A., Parameshachari, B. D., & Lv, J. (2023). Explainable AI for medical image analysis in medical cyber-physical systems: Enhancing transparency and trustworthiness of IoMT. *IEEE Journal of Biomedical and Health Informatics*.

[9] Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare. *Biosensors, 12*(8), 562. https://doi.org/10.3390/bios12080562.

[10] Chen, P.-Y., Cheng, Y.-C., Zhong, Z.-H., Zhang, F.-Z., Pai, N.-S., Li, C.-M., & Lin, C.-H. (2024). Information security and artificial intelligence–assisted diagnosis in an Internet of Medical Thing system (IoMTS). *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3351373.

[11] Kakhi, K., Alizadehsani, R., Kabir, H. D., Khosravi, A., Nahavandi, S., & Acharya, U. R. (2022). The Internet of Medical Things and artificial intelligence: Trends, challenges, and opportunities. *Biocybernetics and Biomedical Engineering, 42*(3), 749–771. https://doi.org/10.1016/j.bbe.2022.05.008.

[12] Sy, I., Diouf, B., Diop, A. K., Drocourt, C., & Durand, D. (2023). Enhancing security in connected medical IoT networks through deep learning-based anomaly detection. In *International Conference on Mobile, Secure, and Programmable Networking* (pp. 87–99). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-52426-4_7.

[13] Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent advances in the Internet-of-Medical-Things (IoMT) systems security. *IEEE Internet of Things Journal, 8*(11), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653.

[14] Alsalman, D. (2024). A comparative study of anomaly detection techniques for IoT security using AMoT (Adaptive Machine Learning for IoT Threats). *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3359033.

[15] Wang, J., Jin, H., Chen, J., Tan, J., & Zhong, K. (2022). Anomaly detection in Internet of Medical Things with blockchain from the perspective of deep neural network. *Information Sciences, 617*, 133–149. https://doi.org/10.1016/j.ins.2022.10.060.

[16] Sargunapathi, R., Vinayagamoorthy, P., Sumathi, P., & Begum, S. S. (2020). Mapping of scientific articles on brain tumors: A scientometric study. *Indian Journal of Information Sources and Services, 10*(2), 26–34. https://doi.org/10.51983/ijiss.2020.10.2.490.

[17] Jain, A., & Babu, K. A. (2024). Role of green buildings in the sustainable development of tier-II cities in India. *Archives for Technical Sciences, 2*(31), 368–378. https://doi.org/10.70102/afts.2024.1631.368.

[18] Roy, S. K., & Mandal, S. (2020). Users' perceptions toward library and library services of IISER Kolkata. *Indian Journal of Information Sources and Services, 10*(2), 44–47. https://doi.org/10.51983/ijiss.2020.10.2.487.

[19] Sungur, Ş., Çömez, M., & Köroğlu, M. (2021). Determination of vitamin K2 content of dairy products produced in Hatay region in Turkey. *Natural and Engineering Sciences, 6*(3), 155–165.

[20] Đurić, N., Stević, S., Đurić, D., & Perišić, M. (2018). Research methodology of railway route Doboj – Zenica, section km 103+500 – Maglaj. *Archives for Technical Sciences, 1*(18), 9–20. https://doi.org/10.7251/afts.2018.1018.009D.

[21] Vinodh Kumar, B., Dhanapal, A., & Tharmar, K. (2019). An analysis of online courses: With special reference to SWAYAM. *Indian Journal of Information Sources and Services, 9*(S1), 19–22. https://doi.org/10.51983/ijiss.2019.9.S1.572.

[22] Tharik, M., Saraswathi, S., & Arumugam, K. (2021). Uncommon mass beaching of *Porpita porpita* (Linnaeus, 1758) in the Gulf of Mannar, Tamil Nadu, India. *Natural and Engineering Sciences, 6*(3), 256–260. https://doi.org/10.28978/nesciences.1036855.

[23] Kalaiselvi, S., & Kumar, R. S. (2024). Experimental investigation on the weld strength of the steel beam with and without stiffener. *Archives for Technical Sciences, 2*(31), 240–247. https://doi.org/10.70102/afts.2024.1631.240.

[24] Dar, B. A., Ahmad, S., & Basharat, M. (2019). Use and awareness of digital information resources (DIRs) by undergraduate students: A survey of Government Degree College for Women Anantnag, Jammu and Kashmir. *Indian Journal of Information Sources and Services, 9*(1), 9–13. https://doi.org/10.51983/ijiss.2019.9.1.604.

[25] Tuncer, S., Koç, H. T., & Erdoğan, Z. (2020). Occurrence of the golden pompano, *Trachinotus ovatus* (Linnaeus 1758) (Osteichthyes: Carangidae) in Dardanelles, the Sea of Marmara. *Natural and Engineering Sciences, 5*(1), 37–44. https://doi.org/10.28978/nesciences.691695.

[26] Snousi, H. M., Aleej, F. A., Bara, M. F., & Alkilany, A. (2022). ADC: Novel Methodology for Code Converter Application for Data Processing. Journal of VLSI Circuits and Systems, 4(2), 46–56. https://doi.org/10.31838/jvcs/04.02.07.

[27] Jakhir, C., Rudevdagva, R., & Riunaa, L. (2023). Advancements in the novel reconfigurable Yagi antenna. National Journal of Antennas and Propagation, 5(1), 33–38. https://doi.org/10.31838/NJAP/05.01.06.

[28] Suneetha, J., Venkateshwar, C., Rao, A.T.V.S.S.N., Tarun, D., Rupesh, D., Kalyan, A., & Sunil Sai, D. (2023). An intelligent system for toddler cry detection. International Journal of Communication and Computer Technologies, 10(2), 5-10. https://doi.org/10.31838/ijccts/10.02.02.

[29] Kankam, Kunrada, Prasit Cholamjiak, and Watcharaporn Cholamjiak. "A modified parallel monotone hybrid algorithm for a finite family of $\mathcal {G} $-nonexpansive mappings apply to a novel signal recovery." Results in Nonlinear Analysis 5.3 (2022): 393-411. https://doi.org/10.53006/rna.1122092.