Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN

3007-3138

Print ISSN

3007-312X

An Enhanced Data Protection and Security based on Machine Learning: Deep Analysis on Threat Mitigation, Challenges in Internet of Medical Things (IoMTs)

Muhammad Atif Imtiaz[1]

School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, NSW 2522, Australia Department of Electronics Engineering, University of Engineering and Technology Taxila, 47050, Pakistan. matif@uow.edu.au

Kamran Razzaq[2]

The University of Northumbria Newcastle, United Kingdom kamran.razzaq@northumbria.ac.uk

M. Aetsam Javed[3]

Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan. SU92-PHCSW-F24-023@superior.edu.pk

Hajra Masood[4]

Bahria University Lahore Campus. hajra.cs@gmail.com

Hoor Fatima Yousaf[5]

Department of Computer Science, Bahria University, Lahore Campus, 54000, Pakistan. hoorfatima.bulc@bahria.edu.pk

Hira Siddique[6]

School of Mathematics and Applied Statistics, University of Wollongong, NSW 2522, Australia. hira@uow.edu.au

Abstract

The Internet of Medical Things (IoMT) plays a vital role with modern technologies and created a wide range of opportunities in numerous industries especially in the medical field. The opportunities not only last from patient empowerment, medical education and training, remote monitoring as well as healthcare collaboration along with customized treatment, and data sharing plans. Wearable health equipment, and quality improvement initiatives are more enhanced with the adoption of IoMT but due to advancement IoMT sometimes faces various challenges regarding interoperability, data privacy and security as well as enhanced infrastructure costs. Due to the sensitivity of the data in the healthcare domain security and privacy become the key issue of (IoMT). This paper aims to address the implications of data fusion in IoMT, as well as the associated security challenges and their potential solutions, which are lacking in the previous studies as mentioned in the literature. Data collected from IoMT devices has a direct impact on the accuracy of predictions because of its quality, quantity, and relevance. Active and Passive attacks and data security breaches are not only disastrous for IoMT but affect the whole healthcare ecosystem. Modern Cloud computing system with IoMT-sensitive data requires more security as the data is stored in the cloud and physical databases require safety from collection to protection. The storage requires to be more enhanced and improved. In this article, numerous challenges are highlighted by implementing the IoMT to the renowned Machine Learning techniques and providing security mechanisms using SDN SDN-based ML model that protects data through the cloud. The standardization of architecture and security measures may improve the detection of security threats and compromises. Detection of threats and malware in cross-platforms is also an important part of future research that can effectively tackle the heterogeneity of the IoMT systems. In advance, IoMT-based system Cryptography and blockchain-based technologies give promising results to increase security. The findings of this research can assist numerous stakeholders in the healthcare ecosystem. The research highlights the security and privacy concerns by providing a comprehensive list of current challenges and future research directions that must be considered while developing sustainable security solutions for the IoMT infrastructure.

Keywords

Security, privacy, Internet of Medical Things, IOMT, MIOT, healthcare systems, survey.

Introduction

The third wave of Internet expansion is thought to be the Internet of Things (IoT). The medical Internet of Things is a collection of Internet-connected devices used to carry out procedures and provide services that aid in healthcare [1]. With the use of tiny wearable devices or implanted sensors. MIOT has become a new e-healthcare technology that gathers patients' essential bodily data and tracks their pathological information. MIOT applications based on wireless body area networks (WBAN) to implantable medical devices, and has demonstrated considerable promise in improving people's health. The Internet of Medical Things (IOMT) is a global network of interconnected medical devices that anybody, anywhere, at any time, can access [2, 3]. Its development and growth are revolutionizing the healthcare sector. In terms of wellness services that inspire millions of people worldwide to adopt healthier lifestyles, the e-health IOMT-based application landscape has taken a stunning lead [4, 5]. In this regard, healthcare services have evolved into user-centered, accurate, pervasive, and customized services, such as 24-hour private healthcare [6, 7].

Due to advancements in microelectronics, materials, and biosensor designs, smart wearable and implantable medical devices have garnered a lot of attention in recent years. However, due to IOMT's quick development, these IOMT-based healthcare systems' security and privacy have frequently gotten little attention. Inadequate security in IOMT healthcare systems can have the following effects. Since its beginnings, the IOMST has been at risk from cyber-attacks. Due to the absence of necessary security protection, various threats and attacks have the potential to cause major catastrophes for both individuals and the network. As a result, IOMST security and administration become very important. The doctor uses his digital signature and access credentials to recover the secure data [8, 9].

Role of IoMT Ecosystem in Healthcare

The suggested system is put into practice with inexpensive hardware and effective software, and it is safe for sending medical records. Data transmission over communication networks is made possible by the Internet of Medical Things (IOMT), an application of the Internet of Things (IoT) in the medical field. By tracking and controlling the body's vital signs, such as blood pressure, temperature, heart rate, and others, IOMT can specifically help residents and senior citizens live better lives. IOMT has emerged as the primary platform for exchanging information and reaching important decisions, therefore ensuring its security and dependability is essential [10]. The below figure 1 represents the Generalize IOMT Architecture.

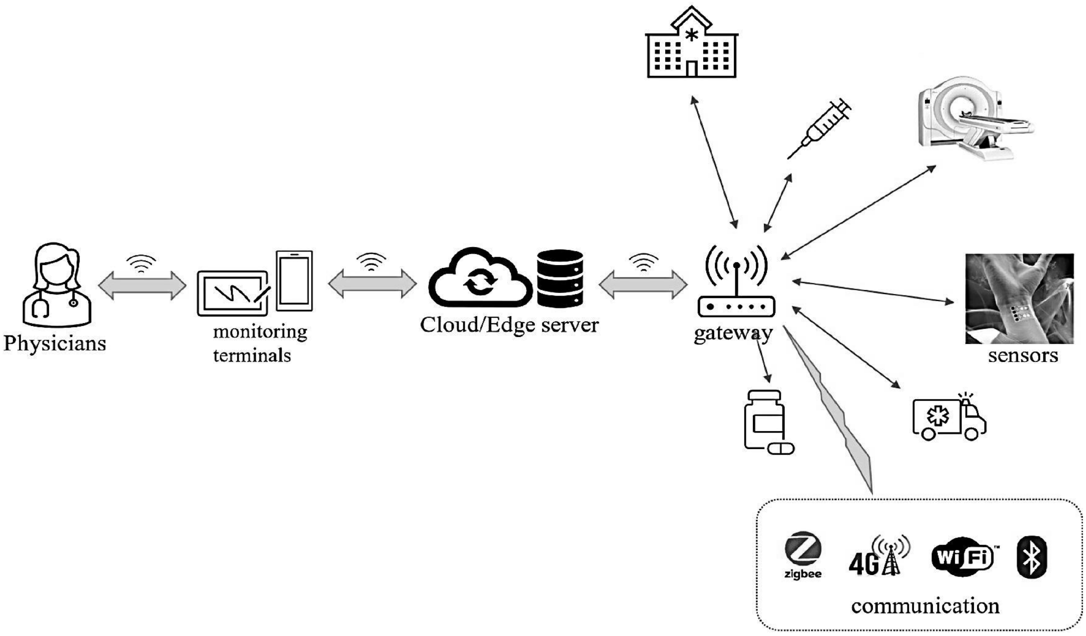


Figure 1: Generalize IOMT Architecture [11]

Many researchers are interested in the growth of IoMT in recent decades. Because IoMT technology is still in its infancy and has not developed sufficiently, there are security issues because of low standards, poor maintenance, and a lack of user education. With malware for ransom, hackers and opponents can quickly take over IoMT devices with inadequate protection. Through unencrypted transmission, hackers can gain access to unencrypted IoMT equipment [12]. IoMT edge networks could seriously jeopardize patient safety and privacy because they are susceptible to a variety of security risks. New security mechanisms are desperately needed to maintain the security of the edge networks to successfully integrate IoMT technology into widespread healthcare systems [13]. Below mentioned table 1 shows a systematic breakdown of IoMT Healthcare Technology.

Table 1: A systematic breakdown of IoMT Healthcare Technology [14]

Area	Method	Characteristics
Leukemia	DenseNet-121	Outstanding performance
Chest X-Ray	Faster R-CNN	Detection accuracy of 97%
Lung CT segmentation	Transfer learning	Promising results
Brain tumor detection	Partial tree algorithm with advanced features	Promising results
Congestive heart failure (CHF)	ANN	Congestive heart failure (CHF)

Services and Role of IoMT Security Architecture in Healthcare

Many of the security schemes created for IoMT devices may also be used to protect medical devices. However, because of their small size and power requirements, wearable and implantable devices are typically constructed with very little funding, and they

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

might not have enough to put those schemes into practice [15, 16]. Figure 2 represents the NDN-based IoMT Security Architecture.

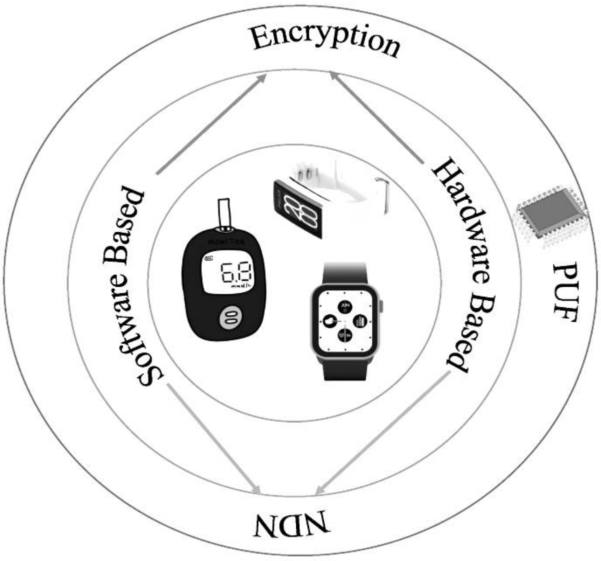


Figure 2: IOMT Security Architecture based on NDN [17]

To ensure the security of this new wave of medical technology, industry, academia, and standards groups must collaborate closely to develop new policies, guidelines, and standards in addition to increasing research into the privacy and security of IOMT device's computational and resource limitations of IOMT devices while maintaining security in IOMT edge networks. We anticipate that this research will contribute to the development and implementation of secure IOMT. The following is a summary of our primary contributions [18].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

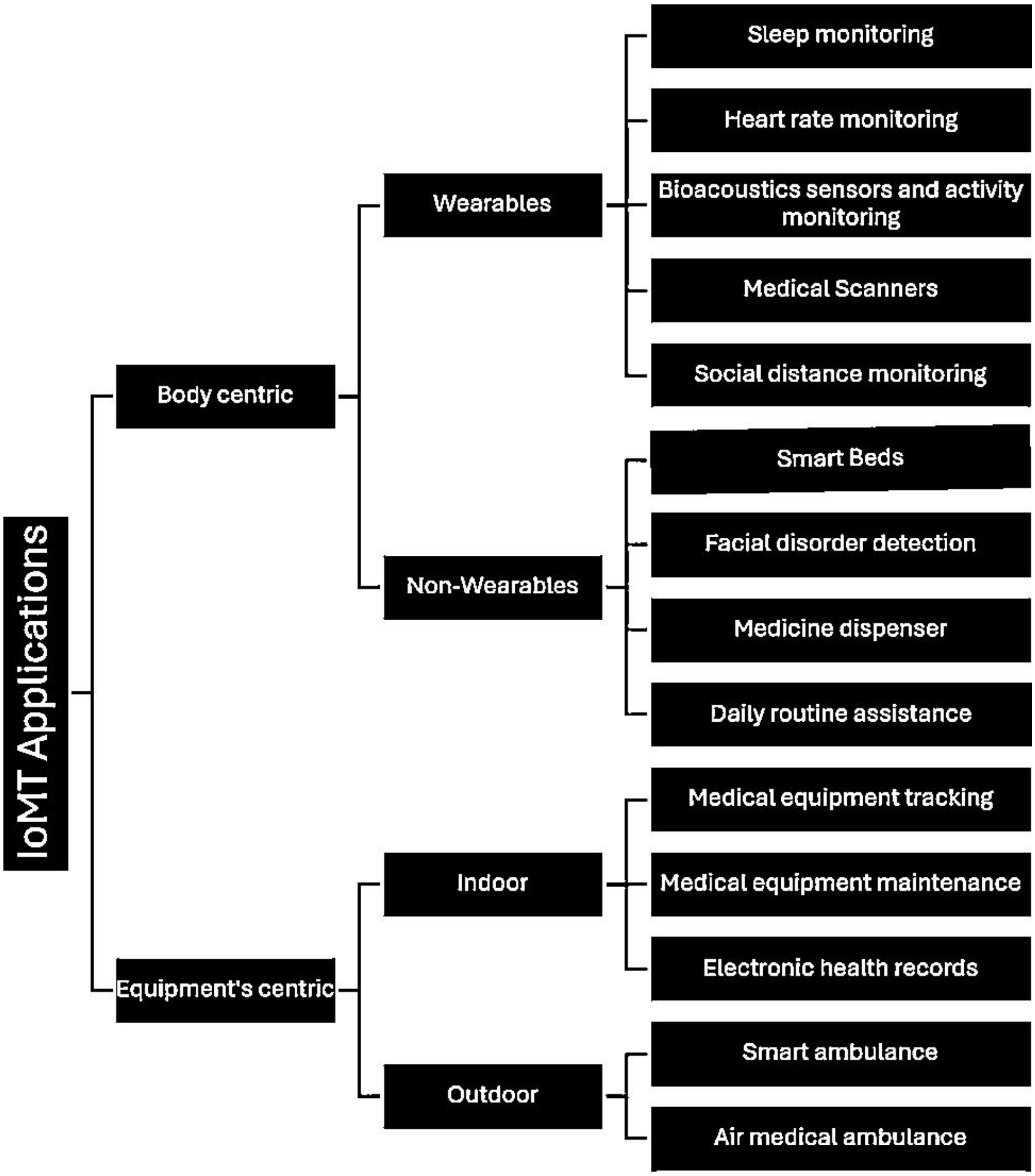


Figure 3: Service-oriented IoMT architecture [19]

Figure 3 shows the numerous Service-oriented without architecture. To design and develop suitable lightweight security mechanisms that overcome the We go over the security specifications required for IOMT systems and the various methods for ensuring safe data gathering as well as storage. We go over the various security methods that are available and how resilient they are to various kinds of attacks. This covers fresh assaults on IoMT systems that have surfaced recently. For the IoMT system, we provide a security

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

architecture that makes use of some of these methods' characteristics. The security of IoMT systems during data collection, transmission, and storage is covered by this framework [20]. The below-mentioned Figure 4 represents the IoT Enhancement with time.

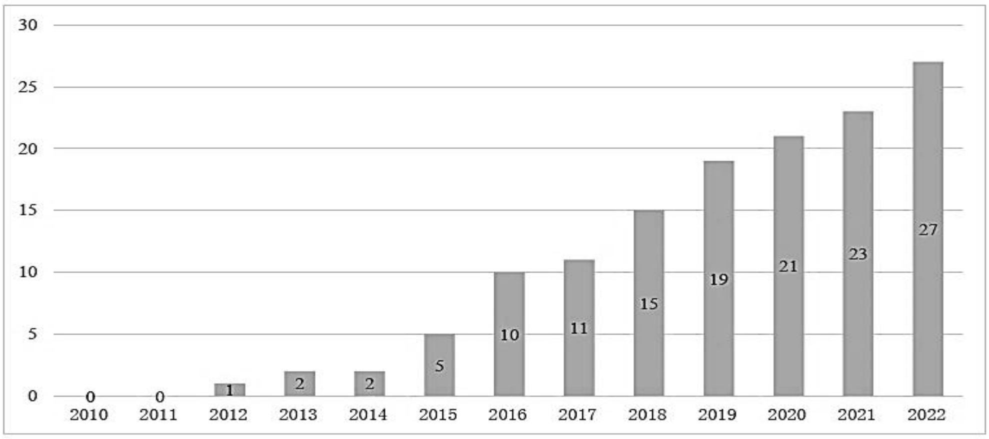


Figure 4: IoT Enhancement with time [22]

Exploratory Data Analysis (EDA)

The Exploratory Data Analysis (EDA) phase of our study was instrumental in uncovering the underlying structure and relationship of the IoMT devices. A component of the larger Internet of Things (IoT), the Internet of Medical Things (IoMT) refers to the collection, storage, and transmission of health data via medical equipment and apps that are connected to the Internet. Through better patient management, diagnosis, treatment, and monitoring, this networked system improves the delivery of healthcare. IoMT includes technologies that help improve patient outcomes and healthcare efficiency, including wearables, sensors, diagnostic equipment, and remote monitoring tools [23, 24]. Table 2 highlights a systematic breakdown of IoMT security risks. To ensure that private information is not shared or made accessible to unapproved parties. Confidentiality in the context of the IOMT edge network refers to safeguarding patient medical information that has been shared with a therapist, doctor, or medical staff from being revealed to unapproved third parties who could endanger the patient or misuse it.

Table 2: A systematic breakdown of IoMT security risks [25]

Challenge	Description	Impact	Examples
Device Vulnerabilities	Limited computational capacity for robust security	Enables hacking and unauthorized access	Insulin pumps, pacemakers
Network Vulnerabilities	Insecure communication protocols between IoMT devices	Eavesdropping and data manipulation	Wi-Fi and Bluetooth
Data Integrity	Unintended data alteration or corruption	Loss of reliable medical records	Sensor data modification

An adversary could, for instance, obstruct communication between the sender (such as a medical IOT device) and the recipient (such as a smartphone gateway) to intercept medical data transmissions and obtain illegal information if the confidentiality of the data is not maintained. There are many different ways to guarantee confidentiality, from physical security to data rendered incomprehensibly by cryptographic methods [26, 27].

IoMT Security Challenges & Authentication in Healthcare

Guarantee that systems function correctly and that authorized users are not denied access to services. As a result, medical data is always available and usable when a genuine organization requests it. Ensuring uninterrupted device and network resource availability when a patient requires care services is crucial in the context of IOMT edge networks [29, 30]. As more resource-constrained medical devices are linked to IoMT-based networks via wireless networks, there is a risk of security breaches by malevolent actors who take advantage of potential flaws in the system to launch attacks, obtain private data, or alter device operations and extract results. The generalized attack types that could potentially target IoMT edge networks are briefly described in this section [31, 32]

Intrusion Detection Threat Mitigation in IoMT

An attack that uses unprotected network connections to obstruct two entities' (like cellphones or sensor nodes') communication without their permission. To obtain valuable information that they can utilize to later pose as the claimant, the attacker surreptitiously listens in on the conversation. Since eavesdropping attacks don't alter network transmission, they are challenging to identify [33]. Figure 5 shows an IOMT architecture for threat mitigations, Intentionally causing a resource or item to behave incorrectly. An attacker might, for example, fabricate the transmission data's sending address to gain unauthorized access to a secure system. Both mimicking and piggybacking are seen as forms of spoofing [34].

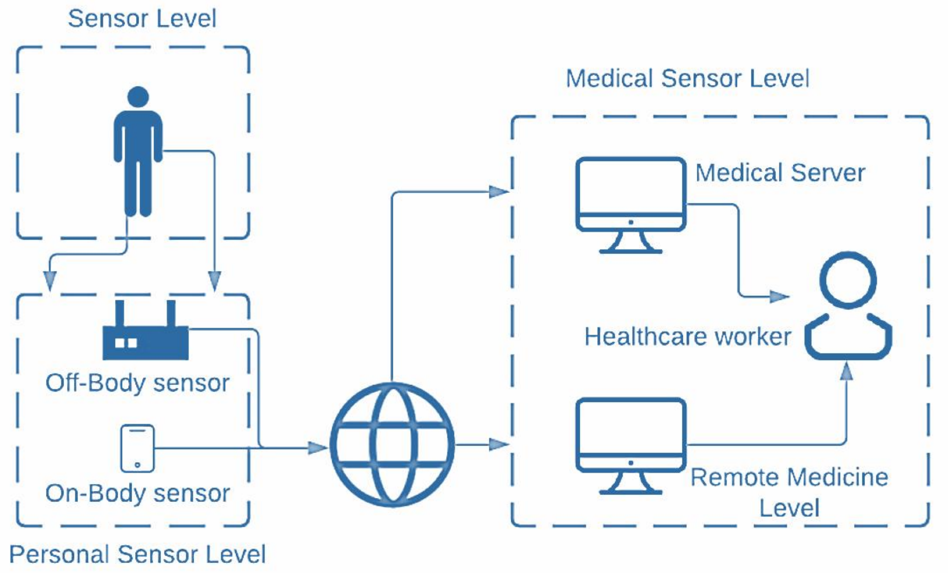


Figure 5. IOMT Architectures for Threat Mitigations [35]

A type of passive attack where an attacker uses observable data flow features to infer information about the transmitted data. For example, when the data is encrypted, the information might not be readable or accessible. These attributes could include the names and locations of the entities participating in the data flow (i.e., its origins and destinations), as well as the presence, absence, amount, direction, frequency, and duration of the flow [36]. An intrusion detection system guarantees that information hasn't been illegally changed or erased. Integrity, when applied to IOMT edge networks, maintains the veracity of patient-related data, including test results, clinical notes, health summaries, and personal medical information [37]. Healthcare businesses now more than ever understand the value of data integrity, especially as a result of the growing reliance on networked data brought about by the integration of developing IoT technology in the healthcare industry. In addition to data integrity, the ideas of device and software integrity have also gained attention in the context of the IOMT edge network.

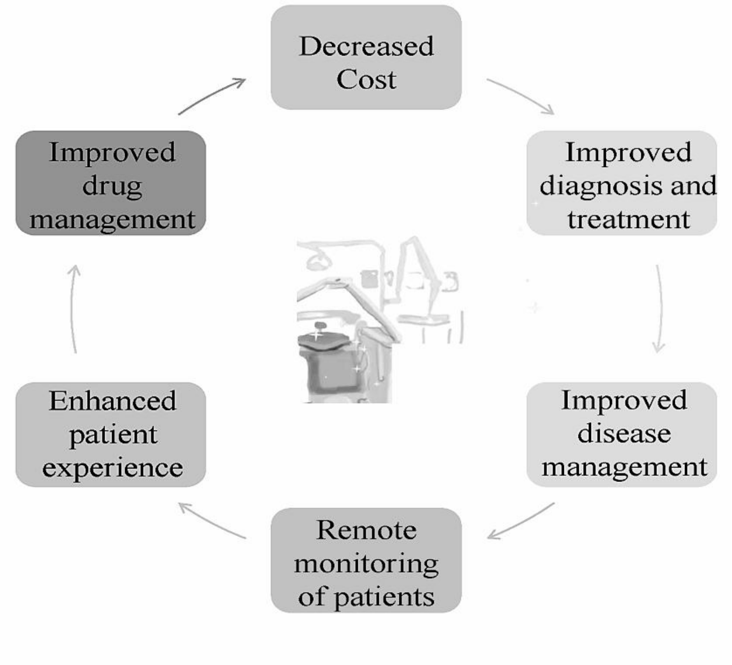

Decreased Cost
Improved diagnosis and treatment
Improved disease management
Remote monitoring of patients
Enhanced patient experience
Improved drug management

Figure 6: Benefits of IoMT Architecture [38]

The integrity of the equipment involved, such as wearable or implanted sensors, is also crucial to the healthcare industry's effective adoption of IoMT edge networks [39]. Stops a party from retracting earlier promises or deeds during a conversation. For example, information taken from a patient's sensors may be sent, but the patient may later claim that the information is not his. Alternatively, a developer with permission may change the firmware in a few sensors and then reject its validity. It is necessary to provide a way to settle conflicts that develop when an entity denies prior commitments or specific approved actions. To settle such disagreements, a certain process including a reliable third party is frequently required [40]. An attacker creates and runs malicious firmware or software to compromise a system's security. This firmware or software is frequently secretly added to another program to erase data, execute harmful or invasive programs, or jeopardize the privacy, correctness, or dependability of the system's data, apps, or operating system as a whole. Malicious mobile code, trojans, worms, and virus programs are common methods of malware attacks, horses, rootkits, or other malicious programs that effectively compromise a system. This type of active attack occurs when a malevolent actor intercepts, compromises, or even hides messages sent back and forth between two authenticated entities (such as the claimant and the authentication protocol verifier). The hacker might change some of the transmitted data to pass for one or more of the relevant legal entities [41].

Synthesis & Evaluation of Intrusion Detection System for IOMT

To find security flaws, test innovative fixes, and assess their effectiveness, this study takes a multidisciplinary approach. The methodology, which focuses on machine learning, blockchain integration, and lightweight cryptography, consists of technical simulations, literature studies, and prototype testing. The following sources were analyzed to ensure a thorough understanding of IoMT security challenges:

Sources: We reviewed 187 articles spanning the period 2010–2022, analyzing topics related to IoMT security, including encryption, authentication, and network vulnerabilities.

Scope: Studies on encryption techniques, blockchain adoption, and AI use in IoMT systems.

Collected data from cybersecurity reports of healthcare organizations experiencing IoMT attacks.

- Notable cases include ransomware in IoT-connected hospital networks and attacks on wearable devices like fitness trackers.
- The security challenges in IoMT were categorized as follows:
- Device Vulnerabilities: Issues in wearable devices and implantable sensors.
- Network Vulnerabilities: Threats during data transmission, such as eavesdropping and unauthorized access.
- Data Integrity Concerns: Risks associated with tampering or loss of sensitive data.

Below mentioned figure 6 represents a Machine Learning based NDN Architecture for IoMT. To evaluate security techniques, a prototype IoMT network was set up comprising simulated medical devices (e.g., heart rate monitors, insulin pumps) and a healthcare cloud platform. Devices equipped with lightweight communication modules (e.g., LoRa, Bluetooth Low Energy).

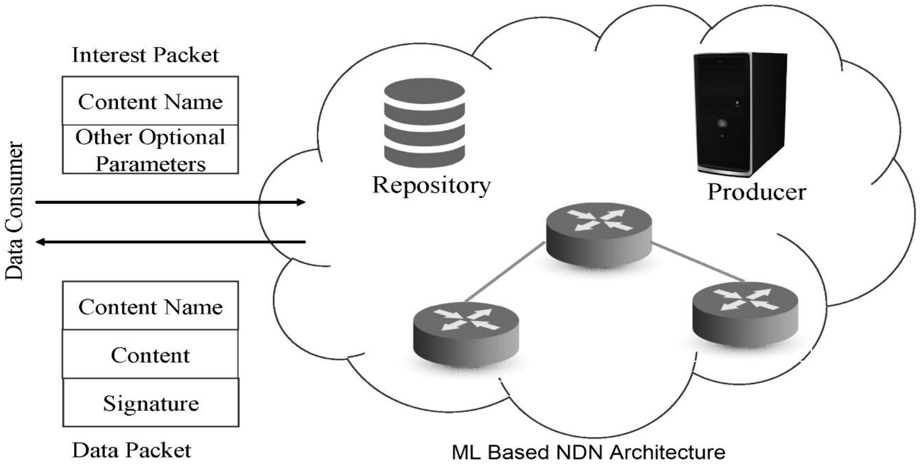


Figure 7: Machine Learning-based NDN Architecture for IoMT Simulated typical patient monitoring scenarios, such as data collection during remote monitoring.

Spectrum of Engineering Sciences

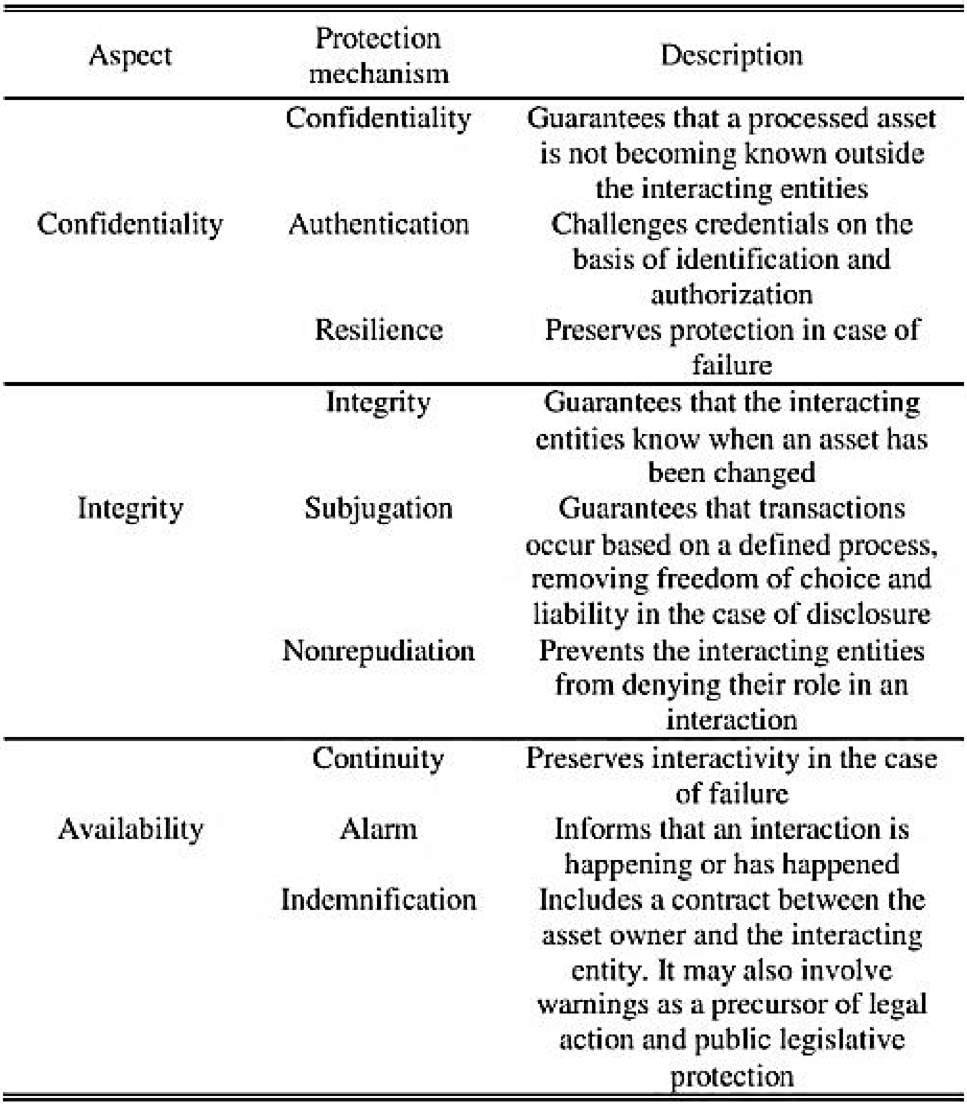
SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

SES

- Security Tests
- Encryption Performance: Compared traditional methods (e.g., RSA) against lightweight alternatives like AES-256 and Elliptic Curve Cryptography (ECC).
- Blockchain Integration: Tested blockchain with decentralized authentication for access control and immutable logging of patient records.
- Anomaly Detection and Developed AI-based models using supervised and unsupervised learning techniques for real-time intrusion detection.

Table 5: Security Aspects for IoMT systems [44]



Aspect	Protection mechanism	Description
Confidentiality	Confidentiality	Guarantees that a processed asset is not becoming known outside the interacting entities
	Authentication	Challenges credentials on the basis of identification and authorization
	Resilience	Preserves protection in case of failure
Integrity	Integrity	Guarantees that the interacting entities know when an asset has been changed
	Subjugation	Guarantees that transactions occur based on a defined process, removing freedom of choice and liability in the case of disclosure
	Nonrepudiation	Prevents the interacting entities from denying their role in an interaction
Availability	Continuity	Preserves interactivity in the case of failure
	Alarm	Informs that an interaction is happening or has happened
	Indemnification	Includes a contract between the asset owner and the interacting entity. It may also involve warnings as a precursor of legal action and public legislative protection

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Machine Learning Based Techniques for Coutner Measure

XGBoost is an ensemble learning method, which means it combines the predictions from multiple models (decision trees) to make a final prediction.

$\hat{y}i=\Sigma(xi)nk=1,\ fk\in F$ Eq (1)

ˆ : is the predicted value of ith instance xi while : is the prediction of the kth tree. :is the feature vector of the ith instance. where ˆ is the prediction and is the target.

$(\theta)=\Sigma l(yi,\hat{y}i)ni=1+\Sigma\Omega(fk)Kk=1$ Eq (2)

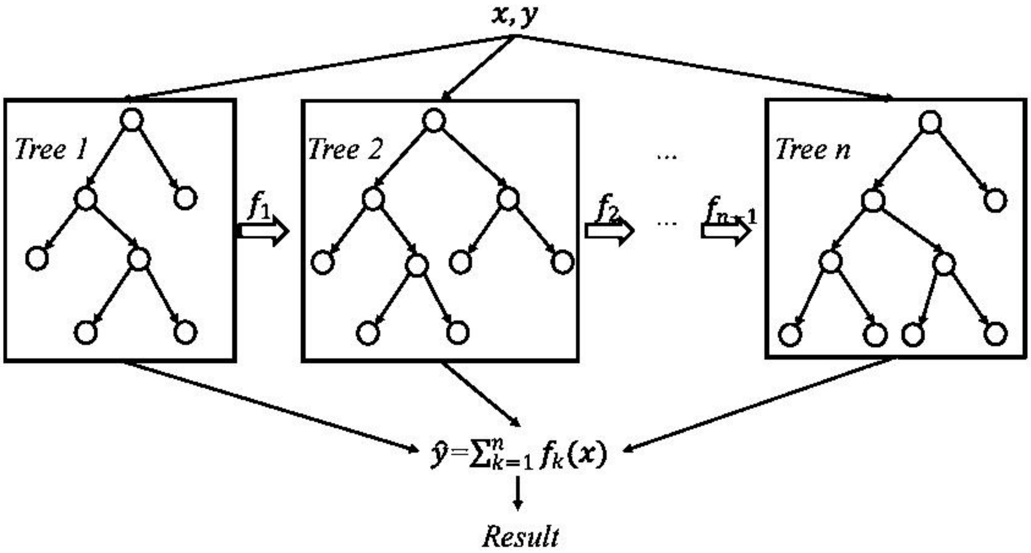


Figure 7. XGBoost Architecture [43]

Naive Bayes is the fast machine learning model which is based on Bayes' theorem. Which predicts the probability of a query belonging to a certain class like malicious or normal, by looking at the various features of data. It works well when features are independent of each other.

$$P(c|x) = \frac{P(X|C).P(C)}{P(X)} \qquad \text{Eq (3)}$$

P (C|X): The probability of which query belongs to the class C malicious.

P (X|C): This is the likelihood the data of X is given to class C.

P (C): This prior probability of the class C is a common class.

P (X): This is the total probability of the data X.

This model is used for baseline because it works fast and is easy to implement. It works well with simple and structured data. A decision tree is a model that splits data based on maximum information gain. Pruning techniques were applied to reduce the overfitting.

$$Gini\ (t) = 1 - \sum_{i-1}^{k} p_i^2 \qquad \text{Eq (4)}$$

t. This is a specific node in the decision tree.

k. The classes of malicious queries in the SQL injection detection.

p_i. The proportion of the elements belonging to class *I* in the node *T*.

We optimized the support vector machine (SVM) with a Radial Basis function kernel for non-linear classification. Hyperparameters C regularization parameter and γ kernel coefficient were fine-tuned using the grid search strategy to achieve the optimal performance. The SVM decision function:

$$f(x) = w^T x + \quad b \qquad \text{Eq (5)}$$

W is the weight of the vector. *X* represents the feature of a vector as an input sample. *b* is the bias term. An ensemble model combining 1,000 decision trees with each tree trained on the bootstrapped samples. The feature important analysis was conducted to optimize the feature selection. A deep neural network with hidden layers, each containing 256 neurons. The dropout and batch normalization were used to prevent overfitting and accelerate convergence.

$$f(x) = max(0, x) \ \ (ReLU) \qquad \text{Eq (6)}$$

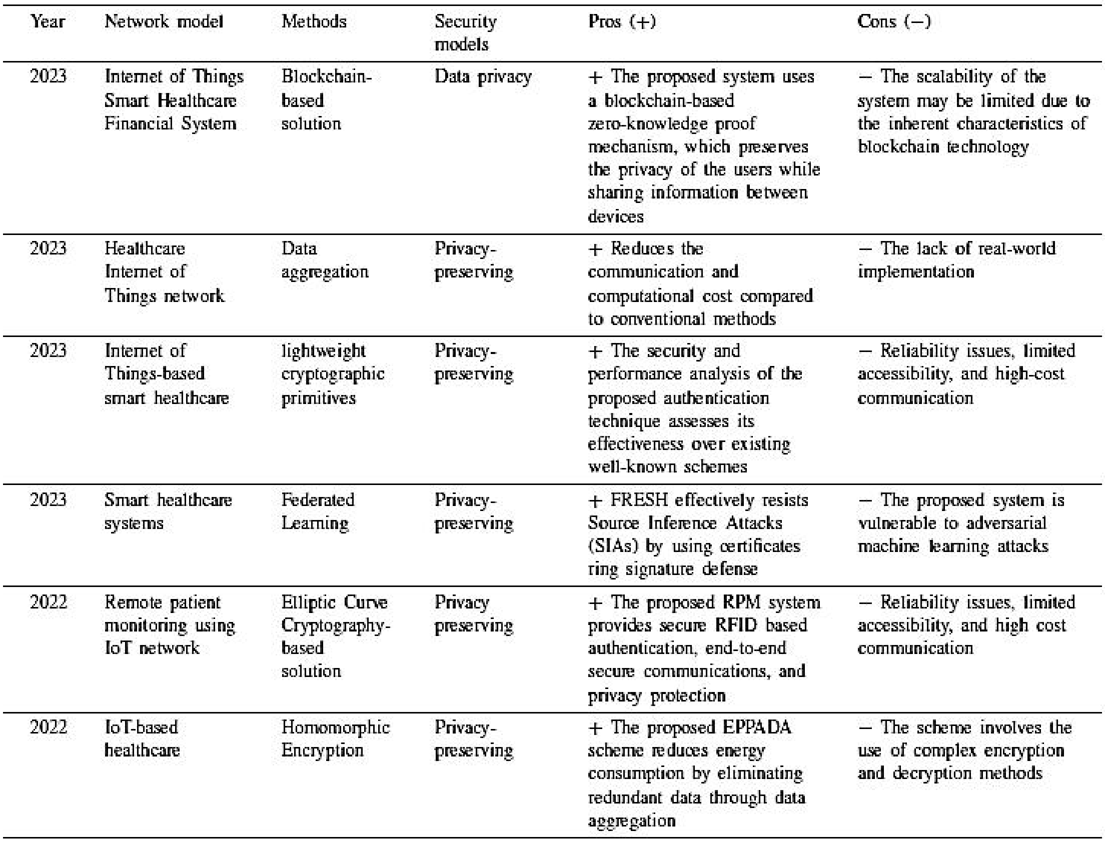
Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Table 6: IoMT security Model Comparison [44]



Year	Network model	Methods	Security models	Pros (+)	Cons (−)
2023	Internet of Things Smart Healthcare Financial System	Blockchain-based solution	Data privacy	+ The proposed system uses a blockchain-based zero-knowledge proof mechanism, which preserves the privacy of the users while sharing information between devices	− The scalability of the system may be limited due to the inherent characteristics of blockchain technology
2023	Healthcare Internet of Things network	Data aggregation	Privacy-preserving	+ Reduces the communication and computational cost compared to conventional methods	− The lack of real-world implementation
2023	Internet of Things-based smart healthcare	lightweight cryptographic primitives	Privacy-preserving	+ The security and performance analysis of the proposed authentication technique assesses its effectiveness over existing well-known schemes	− Reliability issues, limited accessibility, and high-cost communication
2023	Smart healthcare systems	Federated Learning	Privacy-preserving	+ FRESH effectively resists Source Inference Attacks (SIAs) by using certificates ring signature defense	− The proposed system is vulnerable to adversarial machine learning attacks
2022	Remote patient monitoring using IoT network	Elliptic Curve Cryptography-based solution	Privacy preserving	+ The proposed RPM system provides secure RFID based authentication, end-to-end secure communications, and privacy protection	− Reliability issues, limited accessibility, and high cost communication
2022	IoT-based healthcare	Homomorphic Encryption	Privacy-preserving	+ The proposed EPPADA scheme reduces energy consumption by eliminating redundant data through data aggregation	− The scheme involves the use of complex encryption and decryption methods

Discussion

The experimental phase evaluated three main areas: Ensured encrypted medical data could not be intercepted or decoded by unauthorized entities. Evaluated AI algorithms based on the detection of known and unknown threats, generating benchmarks for IoMT systems is presented in Table 5:

Table 5: Benchmarks for IoMT systems [45]

Experiment	Metric	Outcome
AES-256 Encryption	Encryption Latency (ms)	3.5 ms (average)
Blockchain Authentication	Time to Authenticate (ms)	10 ms
AI Model Threat Detection	Detection Rate	92% (Average)

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

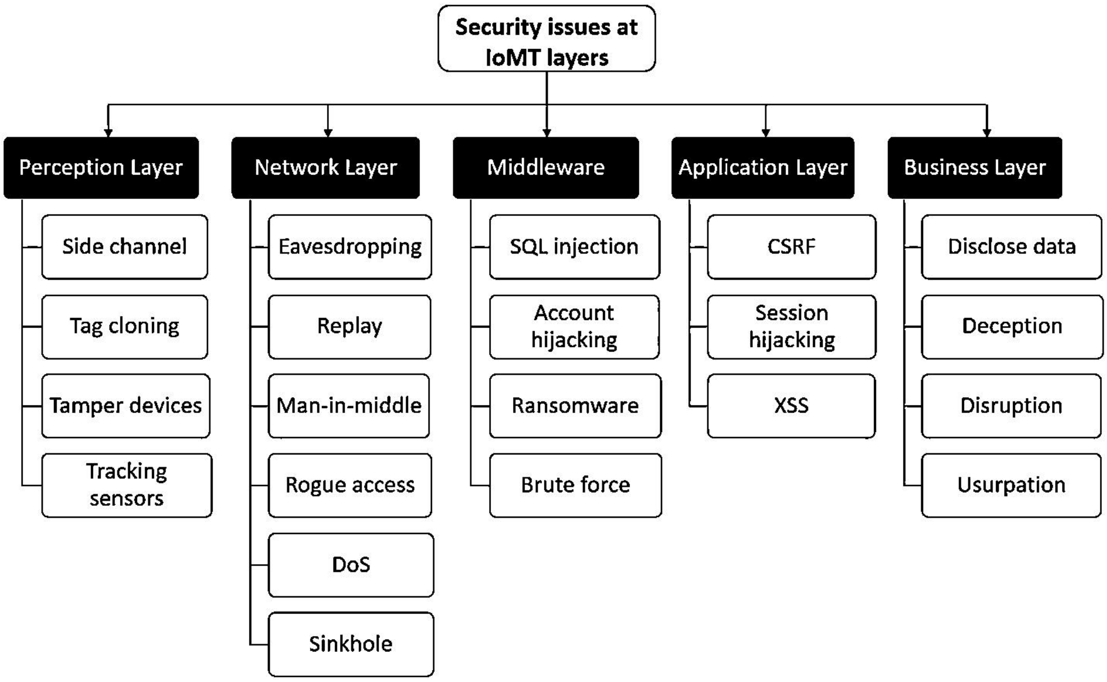


Figure 8: IOMT Architectures with Security Issues [46]

The outcomes of the selection process are first presented in their entirety, followed by individual reports of each research question's findings amount of sensors in our system, and big data problem solving will be put into practice. Patients' medical records will be stored on a private blockchain. This work addresses the issue of IoMT security by presenting a real-time security model with an authenticated encoded encryption technique. The two main concerns facing the IoMT are real-time security and privacy. To encrypt a patient system using a rotational key, we first introduced a run-length encoding technique in this research used a rotating key to decrypt the data and a run-length decoding approach in the physician system. The patient's digital signature guarantees the accuracy of his medical record. Future research will amount of sensors in our system, big data problem solving will be put into practice. Patients' medical records will be stored on a private blockchain. The research paper on the role of IoMT ensures the safety and security of such systems. The development of new procedures, rules, and standards to guarantee the security of this new generation of medical technologies requires strong cooperation between the academic community, industry, and standard organizations due to growing research efforts in the security and privacy of IoMT devices. The paper discusses the methods that give the system session-key agreement, forward/backward secrecy, authentication, authorization, confidentiality, integrity, and key-escrow resilience. By ensuring that these conditions are met, the system can withstand attacks such as physical security tokens, impersonation, manipulation, side channel, sniffer, MITM, relay, brute force, concurrent sessions, clock synchronization, and replay. The following issues could arise, nevertheless, because the methods in this section rely on pre-shared keys or starting arguments. The paper also emphasizes the IOMT devices' network connectivity makes controlling and monitoring them easier, but it also often creates weaknesses in the network and the devices. IOMT devices may be subject to the same security risks and vulnerabilities as other IOT systems and devices. Because IOMT devices manage extremely private health data and some of them have life-sustaining actuation capabilities, security breaches on linked health equipment could directly and potentially kill users.

Conclusion

As the Internet of Medical Things (IoMT) gains ground, the integration with Circular Economy (CE) becomes popular. New business models and services are modeled, materializing, among others, remote sensing, assistance of elder people, and bioinformatics with crowdsourcing and Big Data. In conclusion, numerous software programs and medical gadgets are used to produce vast volumes of data and enhance the quality of medical services. Future related research will focus heavily on how to effectively protect data security and privacy at every stage of data flow. This study addresses the security and privacy concerns from five technological perspectives and outlines the obstacles to further research, beginning with the security and privacy requirements of MIOT. Although MIOT has received a lot of attention, more fruitful research is required since the associated standards and technical specifications particularly those about the unique application requirements of health care are constantly evolving.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.

[2] Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.

[3] Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.

[4] Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.

[5] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[6] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of

Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[7] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[8] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[9] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[10] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[11] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[12] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[13] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[14] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[15] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[16] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[17] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[18] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[19] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[20] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[21] Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in

morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.

[22] Apthorpe, N., Reisman, D. and Feamster, N., 2016. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic, Workshop on Data and Algorithmic Transparency (DAT), New York, USA, 19 November.

[23] Zhou, W. and Piramuthu, S., 2014. Security/privacy of wearable fitness tracking IoT devices, CISTI, IEEE, Barcelona, Spain, 18-21 June, pp. 1-6.

[24] Perera, C., 2017. Privacy guidelines for Internet of Things: a cheat sheet, Technical report, New Castle University, UK, pp. 1-9.

[25] Ferrag, M. A., Shu, L., & Choo, K. R. (2021). Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives. IEEE/CAA Journal of Automatica Sinica, 8(9), 1477-1499. https://doi.org/10.1109/JAS.2021.1004087

[26] What security threats are targeting IoMT devices (and how to prevent being hacked) | Nuspire Last access to the website: 10/05/2024.

[27] Chaudhry, S. A., Irshad, A., Nebhen, J., Bashir, A. K., Moustafa, N., Al-Otaibi, Y. D., & Zikria, Y. B. (2021). An anonymous device to device access control based on secure certificate for internet of medical things systems. Sustainable Cities and Society, 75, 103322. https://doi.org/10.1016/j.scs.2021.103322.

[28] Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access, 7, 135632-135649. https://doi.org/10.1109/ACCESS.2019.2941575

[29] What is an Intrusion Detection System (IDS)? | IBM. Qu'est-ce qu'un système de détection d'intrusion (IDS) ? | IBM Last access to the website: 20/05/2024.

[30] Intrusion Detection System (IDS) – GeeksforGeeks. Intrusion Detection System (IDS) - GeeksforGeeks Last access to the website: 20/05/2024

[31] Baştanlar, Y., Özuysal, M. (2014). Introduction to Machine Learning. In: Yousef, M., Allmer, J. (eds) miRNomics: MicroRNA Biology and Computational Analysis. Methods in Molecular Biology, vol 1107. Humana Press, Totowa, NJ. https://doi.org/10.1007/978-1-62703-748-8_7

[32] Mienye, I. D., & Sun, Y. (2022). A survey of ensemble learning: Concepts, algorithms, applications, and prospects. IEEE Access, 10, 99129-99149. https://doi.org/10.1109/ACCESS.2022.3207287

[33] Shiplu, A.I., Rahman, M.M., Watanobe, Y. (2024). A Robust Ensemble Machine Learning Model with Advanced Voting Techniques for Comment Classification. In: Sachdeva, S., Watanobe, Y. (eds) Big Data Analytics in Astronomy, Science, and Engineering. BDA 2023. Lecture Notes in Computer Science, vol 14516. Springer, Cham. https://doi.org/10.1007/978-3-031-58502-9_10.

[34] Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L. F., & Haskell-Dowland, P. (2021). ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things. Ad Hoc Networks, 122, 102621. https://doi.org/10.1016/j.adhoc.2021.102621.

[35] Ahady, Anar & Ghubaish, Ali & Salman, Tara & Ünal, Devrim & Jain, Raj. (2020). Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. IEEE Access. PP. 10.1109/ACCESS.2020.3000421.

[36] Gupta, K., Sharma, D. K., Datta Gupta, K., & Kumar, A. (2022). A tree classifier based network intrusion detection model for Internet of Medical Things. Computers & Electrical Engineering, 102, 108158. https://doi.org/10.1016/j.compeleceng.2022.108158.

[37] Deborah Oladimeji. (2021). An intrusion detection system for internet of medical things. Dalhousie University. URL: https://dalspace.library.dal.ca/handle/10222/80561.

[38] Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J. C., &amp; Rodriguez, J. (2021). An anomalybased intrusion detection system for internet of medical things networks. Electronics, 10(21), 2562. https://doi.org/10.3390/electronics10212562

[39] Firat Kilincer, I., Ertam, F., Sengur, A., Tan, R.-S., &amp; Rajendra Acharya, U. (2023). Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. Biocybernetics and Biomedical Engineering, 43(1), 30–41. https://doi.org/10.1016/j.bbe.2022.11.005.

[40] Basharat, Asma & Mohamad, Mohd & Khan, Attiya. (2022). Machine Learning Techniques for Intrusion Detection in Smart Healthcare Systems: A Comparative Analysis. 29-33. 10.1109/ICSSA54161.2022.9870973.

[41] Reji, Alan & Pranggono, Bernardi & Marchang, Jims & Shenfield, Alex. (2023). Anomaly Detection for the Internet-of-Medical-Things. 1944-1949. 10.1109/ICCWorkshops57953.2023.10283523.

[42] Ravi, Vinayakumar & Pham, Tuan & Alazab, Mamoun. (2023). Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. IEEE Internet of Things Magazine. 6. 10.1109/IOTM.001.2300021.

[43] Judith, A., Kathrine, G. J. W., Silas, S., & J, A. (2023). Efficient deep learning-based cyber-attack detection for Internet of Medical Things devices. Engineering Proceedings, 59, 139. https://doi.org/10.3390/engproc2023059139Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., &amp; Bhushan, B. (2022).

[44]F Faruqui, N., Yousuf, M. A., Whaiduzzaman, M., Azad, A., Alyami, S. A., Liò, P., Kabir, M. A., & Moni, M. A. (2023). SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization. Electronics, 12(35), 3541. https://doi.org/10.3390/electronics12173541

[45] Shafiq, M., Choi, J. G., Cheikhrouhou, O., & Hamam, H. (2023). Advances in IoMT for healthcare systems. Sensors (Basel), 24(1), 10. https://doi.org/10.3390/s24010010.

[46] Kumar, G., Singh, O.P., & Saini, H. (Eds.). (2021). Cybersecurity: Ambient Technologies, IoT, and Industry 4.0 Implications (1st ed.). CRC Press. https://doi.org/10.1201/9781003145042