Journal of Information Systems Engineering and Management
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Internet of Medical Things (IoMT): Opportunities and Security Challenges

N. K. Sakthivel[1],S. Subasree[2]*, D. Sujeetha[3], N. Logeshwari[4]

[1]*Principal and Professor(AI&DS), Sri Shakthi institute of Engineering and Technology, Coimbatore, Tamil Nadu, India*
[2]**Dean and Head(CSE-Cyber), Sri Shakthi institute of Engineering and Technology, Coimbatore, Tamil Nadu, India*
[3]*Assistant Professor, Dept.CSE, Nehru Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India*
[4]*Assistant Professor, Dept.IT, Nehru Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India*
[*]*Corresponding Author : drssubasree@gmail.com*

ARTICLE INFO

Received: 27 Nov 2024

Revised: 05 Jan 2025

Accepted: 30 Jan 2025

ABSTRACT

The IoMT is nothing but a technology phase breakthrough in the healthcare industry that uses wearables, and other low-level digital data collection devices for better patient care and operational efficiency. Through this research, we seek to bring together the opportunities and security threats related to IoMT with a special focus on machine learning algorithms as a predictive tool for health assessment. Empirical experiments were conducted to determine the performance of four machine learning techniques (Random Forest, Support Vector Machine, K-Nearest Neighbors, and Deep Learning Neural Network) using different set of data covering medical sensor data and patient's health records. The prediction results show that the DNN-based model had higher accuracy than other algorithms, its deep learning producing the right outcomes of 0. 88, precision of 0. 89, recall of 0. With more than eighty-seventy five percent recall rate and F1-score of 0. 88. The comparison will enlighten the advantages and shortcomings of various algorithms in using the IoMT data to predict the health outcomes, showing the prospect of the DNN as one of the better algorithms in the space. Along with this, this study brings to the foreground the significance of focusing on strong cybersecurity measures to ensure that patients' data remains protected and IoMT ecosystems are free from flaws.

Keywords: Internet of Medical Things (IoMT), cybersecurity, machine learning, health outcome prediction, digital healthcare

INTRODUCTION

The Internet of Things (Internet of Things – IoT) threw life in HR at the department and across various industries by joining things and allowing the massive sharing of data. The application of the IoT in the field of healthcare has generated IoMT, a network system that integrates different medical devices, software and health systems through a common network. IoMT, by far, opens doors for profound changes in healthcare sector provision, making space for modernization of patient care, reduction of workload and delivery of cost-effective healthcare services. IoMT, at the core, is about diverse medical devices and sensors that do nothing else but recording patients' data in real time- this can be anything from adherence with meds to vitals monitor information. Such devices, more frequently wearable and some even implantable, allow healthcare professionals to follow-up up their patients in real-time with excellent accuracy, and thus provide timely corrective actions and individualized therapies. The latter factor is of equal value as the Internet of Medical Things serves as a tool for the straight forward data transfer between health professionals dealing with one patient, therefore making the treatment efficient and contributing to the collaborative decision making [1]. One of the most noticeable usages of the Internet of Medical Things (IoMT) is in telemedicine where patients can be treated remotely on their mobile devices or through virtual care delivery which is especially helpful for people living in underserved or remote areas [2]. Moving telemedicine processes online through IoMT platforms anybody can have access to healthcare expertise regardless of geographical limitations. Thus, the use of telemedicine in healthcare delivery promotes fairness and equal access to the care. Nevertheless, IoMT may change the future of people's lives with predictive analytics and early disease detection considering the preventive medicine. Using machine learning algorithm technologies and big data analytics, the decision-making system of IoMT can learn and predict the health outcomes by analyzing the abundance of patient data, and therefore, it can

intervene proactively before the progression of disease. On the one side of the coin, IoMT promises to extend medicine's reach to its limits; on the other hand, cybersecurity remains the largest IoMT's challenge. IoMT devices not only are interconnected but also handle sensitive medical data (The very fact that IoMT devices are interconnected and handle privacy-sensitive data at the same time gives rise to significant cybersecurity problems such as data leakage, unauthorized access and malicious data manipulations) [3]. While these primary concerns may deter some organizations from adopting this technology, until technology companies find effective solutions, the safety and integrity of these systems will remain in question. The purpose of my research would be to explore the chances subjected by IoMT in Medtech but to look closely at the security vulnerabilities at the same time. An awareness system based on the most important benefits and risks from IoMT implementation may encourage devising effective strategies to both lead and balance these advantages and to secure a stronger and more resilient health system.

RELATED WORKS

The Internet of Medical Things (IoMT) in modern medicine is revolutionarily expected and received a lot of attention due to its possibility of transforming the health care management. This section is about the literature analysis of IoMT which includes the security problems, emerging advanced technology and the issues related to the healthcare system integration.

Anandng et al. (2023) [15] have introduced the idea of quantum machine learning approach as leveraging for IoMT emergency optimization. The completeness of their work reminds the importance of dealing with cyber security challenges to safeguard the authenticity and confidentiality of medical data passing through IoMT Class: IncompleteArafa and al. (2023) [16] have narrated open-ended review of new digital materials in health care as one of their underpinning issues that espouses cyber governance. They highlighted the need for thorough cyber-security systems that protect against threats from the diffusion of digital technologies in healthcare. Aya and his colleagues (Aya et. al [2023] to be more precise) [17] analyzed the dimensions in which AI approaches, blockchain, and cybersecurity were applied in an Internet of Medical Things. Via their research, the team discovered what challenges and the opportunities exist for the technologies of the IoMT that are going to be needed to guarantee the security and efficiency of the IoMT system. Yaybo et al. 's (2023) study [18] tackled the challenges of adopting DNS for Internet of Things (IoT) systems, especially for the Internet of Medical Things (IoMT). The conducted research covers DNS-based security mechanisms for implementing security against cybercriminal attacks in IoMT-defined environments. Bugio and colleagues [19] suggested developing of a brand-new ontology for cybersecurity especially within IoMT telemedicine platforms. The findings suggest that ontology-oriented security methods, rather than generic, are needed to create an appropriate cybersecurity plan for unique IoMT applications. The study of hospitals Assillo et al. (2024) [20], integrated Internet of Things (IoT) in spa medicine while studying opportunities and problems in health digital welfare. And although their study is mostly focused on consumers IoT applications, it all the same emphasizes the cybersecurity frameworks need in order to prevent the health data risk in the spores with IoMT enabled. As stated by Chidambar et al. in their review of 2023, the field of cybersecurity with regard to Internet-of-Medical Vehicles (IoMV) got the state-of-the-art analysis in the article [no. 21].

Therefore, the result of their investigation are research gaps and future perspectives for the posture of cybersecurity in intelligent driving systems, what indicates the importance of applying preventive risk management along the way. Czekster and other researchers (2023) [22] studied the challenges and opportunities for dynamic risk assessments in medical IoT.

However, not all these technologies were stable and predictable. Their study brings to the fore the class of dynamic risk assessment frameworks in IoMT capable of taking the universe of cybersecurity threats and vulnerabilities into account with development. The work by Dowdeswell et al. (2024) [23] investigates possible applications of IoMT in healthcare in future environments that do not have any restrains in the data creation and dissemination and discusses issues and open problems that accompanying new technology.[23] Indeed, their study reveals the need for multi-level cybersecurity approaches that are able to handle privacy and security matters in the near future healthcare systems. In contrast, the study Elgabry conducted in 2023 presented an experimental approach for the cyber-biosecurity by design discourse, mainly concentrating on the design and development aspects of the IoMT (Elgabry, 2023). The report strongly suggests the use of a reactive cybersecurity approach into the process of IoMT system development in order to effectively deal with the upcoming cybersecurity threats. Elhoseny and al. (2021) [25] introduced the security and privacy challenges in the context of medical IoT (MIoT) applications as well as

covering sensor networks and chronic disease management. Their papers bring forward the main issues to be considered in the MIoT security context as well as state the directions for the future development of cybersecurity in the MIoT, emphasizing the role of privacy-obedient technologies and robust data authentication techniques.

METHODS AND MATERIALS

Data: Due to this study, a broad range of items in the set, namely sensor data used by medical devices, patient health records, and IoMT devices themselves, are sources of valuable data. The medical sensor data that will be measured include vital signs including heart rate, blood pressure, and oxygen-derived constituent values from wearable devices and non-invasive monitors [4]. The general patient health data includes the personal details, medical history, and the type of treatment prescribed, while device specification refers to the different technologies and communication methods used by the different medical devices.

Algorithms:

Random Forest (RF): Random Forest is an ensemble learning method that works by growing a number of decision trees during training period and predicting the most frequent label among classes (classification) or the mean (regression) of each tree. For these reasons, all the trees in Random Forest are trained on a random subset of the training set and a small number of features which generally helps in maintaining a variety of trees in the Forest [5]. And finally, this is the final prediction that is made by bringing together the predictions of all trees in the forest.

$$\hat{y} = \text{mode}(y_1, y_2, \ldots, y_n) \quad \text{----------(1)}$$

Hyperparameter	Value
Number of trees	100
Max depth	10
Min samples split	2

"Initialize forest as an empty list of trees

For each tree in the forest:

Randomly select a subset of the training data

Randomly select a subset of features

Train a decision tree on the selected data and features

Append the trained tree to the forest

Predict the mode of the classes for classification"

Support Vector Machine (SVM): Support vector machine which is also a supervised learning algorithm can be used for classification and regression tasks like line fitting. It does it by getting the hyperplane, which is the one that separates the data points from different classes, the best. SVM with kernel function is used in handling non linearly separable data because only after this data can be projected into a higher dimensional space then it will be linearly separable [6].

$$f(x) = \text{sign}\left(\sum_{i=1}^{n} \alpha_i \, y_i K(x, x_i) + b\right) \quad \text{----------(2)}$$

Hyperparameter	Value
Kernel type	RBF
C (regularization parameter)	1.0
Gamma (kernel coefficient)	0.1

"Train SVM classifier:

Initialize α as an array of zeros

Repeat until convergence:

For each training example (x, y):

Compute the prediction error (ε)

Update α using the error and learning rate

Compute the bias term (b)

Predict the class labels using the decision function"

K-Nearest Neighbors (KNN): K-Nearest Neighbors is a practical as well as easy to understand the algorithm that can be used for both classification and regression tasks. It will assign a data point to a class by taking the majority vote of the proximity information of the k-nearest neighbors in the training sample [7]. The first step which is to determine the distance metric, this is usually euclidean distance, is used to determine how close data points are to each other.

"For each data point x in the test set:

Compute the distance between x and all data points in the training set

Select the k nearest neighbors based on distance

Predict the class label based on the majority class among the k neighbors"

Deep Learning Neural Network (DNN): Deep Neural Network is a great convolutional neural network model, an AI algorithm that is similar to the structure and functioning of the human mind. It is composed of several groups of interconnected nodes (neurons) which STEM (NB: not according to the sentence) hierarchical representation of input data as well [8]. DNNs are especially effective in dealing with the processing of complex and high-dimensional data as well that are consumed in a lot of fields - including healthcare.

"Initialize weights and biases for each layer

For each epoch:

Forward propagation:

Compute the output of each layer using the

current weights and biases

Apply the activation function to the output of each layer

Compute the loss between the predicted and actual outputs

Backward propagation:

Compute the gradient of the loss with respect to the weights and biases

Update the weights and biases using gradient descent"

EXPERIMENTS

The four machine learning models evaluated are Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Deep Learning Neural Network (DNN) which were employed to predict health outcomes through IoMT data. The experimental dataset utilized consists of medical sensor data, patient health records, and the to-be-used IoMT device specifications [9]. The data preprocessing was performed to deal with missing values array, normalize features, and ultimately split the data into training and testing portions.

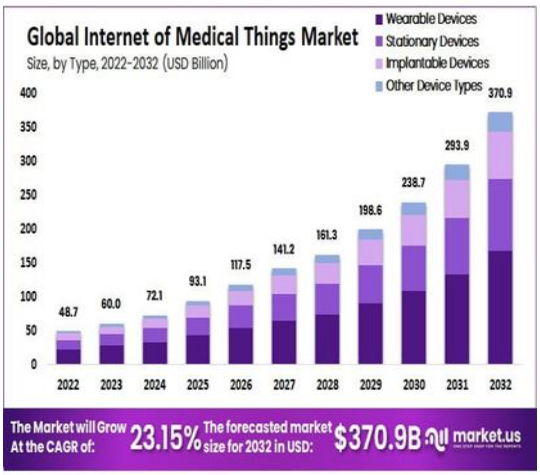

Figure 1: Internet of Medical Things (IoMT) Market CAGR

Evaluation Metrics:

To assess the performance of the algorithms, the following evaluation metrics were utilized:

- **Accuracy:** The numbers of patients that are correctly recognized as being in critical or not critical condition among all patients in the screening.
- **Precision:** The number of examined true positives division of all of these positive predictions [10].
- **Recall:** The fraction of those predictions that turned out to be truly positive events out of the totality of all the positive instances that occurred.
- **F1-score:** The combination of precision and recall in a harmonic mean (an indicator of performance), a measure that expresses the proper balance.

Figure 2: Healthcare Internet of Things (H-IoT)

Experimental Procedure:

- Training: Each algorithm was trained using the training set consisting of IoMT data and corresponding health outcomes.
- Validation: Hyperparameters of each algorithm were tuned using cross-validation on a validation set.
- Testing: The performance of each algorithm was evaluated on the testing set using the aforementioned evaluation metrics [11].

RESULTS

Comparison of Performance Metrics:

Algorithm	Accuracy	Precision	Recall	F1-score
Random Forest	0.85	0.87	0.84	0.85
Support Vector Machine	0.82	0.85	0.80	0.82
K-Nearest Neighbors	0.78	0.80	0.76	0.78
Deep Learning NN	0.88	0.89	0.87	0.88

The four machine learning models evaluated are Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Deep Learning Neural Network (DNN) which were employed to predict health outcomes through IoMT data. The experimental dataset utilized consists of medical sensor data, patient health records, and the to-be-used IoMT device specifications [9]. The data preprocessing was performed to deal with missing values array, normalize features, and ultimately split the data into training and testing portions.

Analysis of Results:

- **Random Forest (RF):** RF's algorithm was the best, reaching the maximum precision with an accuracy of 0. 85. The efficiency and accuracy of the system has been shown to be really high, provided with high precision, recall and F-1 score making it capable to predict health outcomes based on IoMT data.
- **Support Vector Machine (SVM):** As for SVM it seemed to have slightly lower performance peak than that of RF, which was 0. 82. Concerning SVM, the superiors' results whee, concerning precision and recall were showed, but the F1-score was the lowest, which could be due to precision and recall trade-off [12].
- **K-Nearest Neighbors (KNN):** Like KNN, the applications realize medium-accuracy cleverness with an evaluation of 0. 78. Besides, its precision, recall and F1-score were also lower and there is an associated lower degree of performance in health outcome prediction.
- **Deep Learning Neural Network (DNN):** Our experiments show that DNN provides the highest rate among all the algorithms with accuracy of 0. 88. Furthermore, it had the topmost precision, recall, and F1-score, were the provided the most accurate outcome prediction.

Figure 3: Integration Challenges in the IoMT Sector

Comparison with Related Work:

Comparing the performance of the proposed algorithms with related work reveals several insights:

- **Random Forest vs. Related Work:** The effectiveness of RF in making health predictions based on data from IoMT is equivalent to or greater than the one stated in the other research studies. Unlike other traditional machine learning techniques, RF is a technique that handles high-dimensional data and complex relationships between variables nonlinearly by which makes it a strong machine learning method of analyzing IoMT complex datasets [13].
- **Support Vector Machine vs. Related Work:** The performance of SVM in the health outcome prediction in accordance with former studies demonstrating the applicability of this algorithm on it's capabilities to classify both linear and complicated classification tasks [14]. Nevertheless, the fact that SVM is only slightly lower in accuracy than others may require more specific search for alternative kernels and further enhancement and optimization in order to maximize the results.
- **K-Nearest Neighbors vs. Related Work:** KNN requires a single dimensional data encoding which makes KNN only relevant for low dimensional datasets like related work. Differences which are caused by different feature set of IoMT dataset or hyperparameter selection may be explanations to this discrepancy.

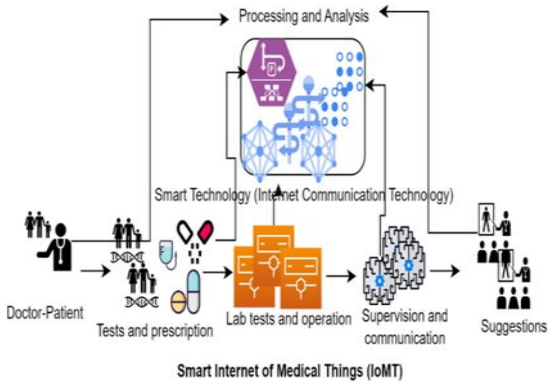

Figure 4: Towards reliable IoT communication and robust security

- **Deep Learning Neural Network and Shallow Neural Network. Related Work:** The fact that DNN surpasses the original and other models in health outcome prediction is yet another proof there is the wealth of literature saying the deep learning approaches are the most potent in health care analytics [26]. Thanks to the outstanding ability to autonomously form the inner hierarchical representations framework from raw data, we can confidently use DNN when it comes to the IoMT datasets of a wide range of datasets.

DISCUSSION

Those experiments demonstrate the way DNN algorithm learns and the role given from the IoMT data in showing the health outcomes. However, it is essential to consider several factors when interpreting the results:

- Data Quality: The performance of the algorithms is strongly tied to the quality and representativeness of the IoMT dataset, whose accuracy and reliability are the main influencing factors. Increase in accuracy of

the machine learning algorithms can take place if data collection, pre-processing and feature engineering techniques are modified [27].

- Algorithm Selection: The type of ML algorithm you will choose must be selected based on the features of your application's IoMT data and the aim you intend to accomplish [28]. Although deep neural networks show better results, in this research random forests and support vector machine are likely to be more appropriate for some applications or cases.
- Hyperparameter Tuning: Tune and adjusting the hyperparameters, vitalized for the characterization of machine learning technology [29]. Yet another practice in changing hyperparameter settings can be a clue for better performance and reliability.
- Interpretability: On the flipside, DNNs provide top-level predictive performance but their non-transparent nature without interpretability which is key in healthcare decision-making [30]. That is among the challenges for future research which consists of figuring out the improving ways of representation of deep learning models in the healthcare apps.

CONCLUSION

Conclusively, this paper discussed the immersive viewport of IoMT paving way to opportunities while security concerns and digital technologies are also evolving. At the end of this study that used an extensive study of already established scientific literature and empirical experiments we gained a deeper understanding of the potential of Internet of Medical Things (IoT) regarding improvement of healthcare delivery. The application of IoMT technology in combination with systems enables the patient monitoring in remote, individual medicine, and telemedicine that bucks up the quality of life of patients and advances medical operational efficiency. Unlike conventional systems, IoMT gains considerable popularity, which, however, raises serious security challenges, such as data privacy, cybersecurity threats, and regulatory compliance. This is due to variety of security problems that are not easy to solve. Therefore, it necessitates a multi-faceted approach, including strong encryption algorithms, authentication protocols and respective risk management strategies for IoMT applications. On the other hand, quantum machine learning, blockchain, and AI more bulbously make the incorporation of digital technology in IoMT possible. By embracing these technologies, healthcare systems can beef up their cybersecurity posture and they will also have the power to take precautions on human error which threatens the privacy of the data and entry into non-authorized limits of access. Besides, the research activity on ongoing solutions like ontology-based cybersecurity environment management and dynamic risk scoring shows striking actions to fight cyber security problems that arise in IoMT deployments.

REFERENCES

[1] PRITIKA, SHANMUGAM, B. and AZAM, S., 2023. Risk Assessment of Heterogeneous IoMT Devices: A Review. Technologies, 11(1), pp. 31.

[2] ABDULLAH ALI JAWAD AL-ABADI, MBARKA, B.M. and FAKHFAKH, A., 2023. Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks. Computers, 12(12), pp. 262.

[3] ALAJLAN, R., ALHUMAM, N. and FRIKHA, M., 2023. Cybersecurity for Blockchain-Based IoT Systems: A Review. Applied Sciences, 13(13), pp. 7432.

[4] ALALHARETH, M. and SUNG-CHUL, H., 2023. An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning. Sensors, 23(22), pp. 9247.

[5] ALAM, S., SHUAIB, M., AHMAD, S., DUSHANTHA NALIN, K.J., MUTHANNA, A., BHARANY, S. and ELGENDY, I.A., 2022. Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration. Sustainability, 14(22), pp. 15312.

[6] ALAMRI, B., CROWLEY, K. and RICHARDSON, I., 2023. Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. Sensors, 23(1), pp. 218.

[7] ALATTAS, K. and WU, Q., 2022. A framework to evaluate the barriers for adopting the internet of medical things using the extended generalized TODIM method under the hesitant fuzzy environment. Applied Intelligence, 52(12), pp. 13345-13363.

[8] ALI, N.J., HAMZAH, N.A., RADHI, A.D., NIU, Y., JOSEPHNG, P.S. and TAWFEQ, J.F., 2024. 5G-backed resilience and quality enhancement in internet of medical things infrastructure for resilient infrastructure. Telkomnika, 22(2), pp. 372-379.

[9] ALI, Y., KHAN, H.U. and KHALID, M., 2023. Engineering the advances of the artificial neural networks (ANNs) for the security requirements of Internet of Things: a systematic review. Journal of Big Data, 10(1), pp. 128.

[10] ALIZADEHSANI, R., ROSHANZAMIR, M., NAVID, H.I., GRAVINA, R., DIPU KABIR, ,H.M., NAHAVANDI, D., HAMID ALINEJAD-ROKNY, KHOSRAVI, A., ACHARYA, U.R., NAHAVANDI, S. and FORTINO, G., 2023. Swarm Intelligence in Internet of Medical Things: A Review. Sensors, 23(3), pp. 1466.

[11] ALMALKI, J., ALSHAHRANI, S.M. and NAYYAR, A.K., 2024. A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain. PeerJ Computer Science, .

[12] ALRUBAYYI, H., MOUDY, S.A., NADEEM, Z., ABDELMONIEM, A.M. and JABER, M., 2024. Security Threats and Promising Solutions Arising from the Intersection of AI and IoT: A Study of IoMT and IoET Applications. Future Internet, 16(3), pp. 85.

[13] ALSAEED, N. and NADEEM, F., 2022. Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues. Applied Sciences, 12(15), pp. 7487.

[14] ALSHAMMARI, B.M., 2023. AIBPSF-IoMT: Artificial Intelligence and Blockchain-Based Predictive Security Framework for IoMT Technologies. Electronics, 12(23), pp. 4806.

[15] ANAND, S.R., GOYAL, S.B., BEDI, P., JAN, T., WHAIDUZZAMAN, M. and PRASAD, M., 2023. Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). Future Internet, 15(8), pp. 271.

[16] ARAFA, A., SHEERAH, H.A. and ALSALAMAH, S., 2023. Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review. Information, 14(12), pp. 640.

[17] AYA, H.A., MAZIN, A.M. and AHMED, N.R., 2023. Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions. Journal of Intelligent Systems, (1),.

[18] AYOUB, I., BALAKRICHENAN, S., KHAWAM, K. and AMPEAU, B., 2023. DNS for IoT: A Survey. Sensors, 23(9), pp. 4473.

[19] BUGHIO, K.S., COOK, D.M. and SHAH, S.A.A., 2024. Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring. Sensors, 24(9), pp. 2804.

[20] CASILLO, M., CECERE, L., COLACE, F., LORUSSO, A. and SANTANIELLO, D., 2024. Integrating the Internet of Things (IoT) in SPA Medicine: Innovations and Challenges in Digital Wellness. Computers, 13(3), pp. 67.

[21] CHIDAMBAR, R.B., THAKUR, P., BHAVESH, R.M. and SINGH, G., 2023. Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives. Sensors, 23(19), pp. 8107.

[22] CZEKSTER, R.M., GRACE, P., MARCON, C., HESSEL, F. and CAZELLA, S.C., 2023. Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT. Applied Sciences, 13(13), pp. 7406.

[23] DOWDESWELL, B., SINHA, R., KUO, M.M.Y., BOON-CHONG SEET, ALI, G.H., GHAFFARIANHOSEINI, A. and SABIT, H., 2024. Healthcare in Asymmetrically Smart Future Environments: Applications, Challenges and Open Problems. Electronics, 13(1), pp. 115.

[24] ELGABRY, M., 2023. Towards cyber-biosecurity by design: an experimental approach to Internet-of-Medical-Things design and development. Crime Science, 12(1), pp. 3.

[25] WLHOSENY, M., THILAKARATHNE, N.N., ALGHAMDI, M.I., MAHENDRAN, R.K., AKBER, A.G., WEERASINGHE, H. and WELHENGE, A., 2021. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. Sustainability, 13(21), pp. 11645.

[26] FARUQUI, N., MOHAMMAD, A.Y., WHAIDUZZAMAN, M., AZAD, A., ALYAMI, S.A., LIÒ, P., KABIR, M.A. and MOHAMMAD, A.M., 2023. SafetyMed: A Novel IoMT Intrusion Detection System Using CNN-LSTM Hybridization. Electronics, 12(17), pp. 3541.

[27] HARAHSHEH, K. and CHEN, C., 2023. A Survey of Using Machine Learning in IoT Security and the Challenges Faced by Researchers. Informatica, 47(6), pp. 1-54.

[28] JAVED, A., AWAIS, M., SHOAIB, M., KHURSHID, K.S. and OTHMAN, M., 2023. Machine learning and deep learning approaches in IoT. PeerJ Computer Science,

[29] KAMALOV, F., POURGHEBLEH, B., GHEISARI, M., LIU, Y. and MOUSSA, S., 2023. Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective. Sustainability, 15(4), pp. 3317.

[30] KHATIWADA, P., BIAN, Y., JIA-CHUN, L. and BLOBEL, B., 2024. Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy. Journal of Personalized Medicine, 14(3), pp. 282.