LAUTECH Journal of Computing and Informatics (LAUJCI) – ISSN : 2714-4194
Volume 4. No.1, March 2024 – www.laujci.lautech.edu.ng

A Review on Attack Landscape and Machine Learning Techniques for the Classification of Attacks in Internet of *Medical Things* (IoMT)

Olomu J. O.
Postgraduate Researcher,
Department of Computer Science
Al-Hikmah University, Ilorin, Nigeria
luability4u@gmail.com

Oyelakin A. M.
Lecturer, Department of Computer Science, Crescent University, Abeokuta, Nigeria
moruff.oyelakin@cuab.edu.ng

Ayinla O. M.
Postgraduate Researcher,
Department of Computer Science
Al-Hikmah University, Ilorin, Nigeria
ayinlamutiu2019@gmail.com

Ibrahim H. A.
Postgraduate Researcher,
Department of Computer Science
Al-Hikmah University, Ilorin, Nigeria
igehabiba@gmail.com

ABSTRACT
Healthcare systems globally are struggling to handle the increasing number of patients, partly due to busy work schedules. To address this issue and enhance healthcare services, the Internet of Medical Things (IoMT) is gaining popularity. IoMT refers to internet-connected devices used in healthcare processes. However, the widespread adoption of IoMT devices has led to new security vulnerabilities and cyber threats. Protecting these devices from cyberattacks is vital for patient safety and data integrity. This study focuses on examining trends in cyber-attacks and the use of machine learning for attack classification in the Medical Internet of Things. The research involved a comprehensive analysis of relevant articles written in English between 2016 and 2023. The study established a search strategy and exclusion criteria to identify highly relevant works from reputable research databases. A significant number of papers were carefully chosen, organized, and reviewed. The reviewed articles delve into the threat landscape and assess the strengths and limitations of machine learning-based techniques for classifying security attacks in IoMT systems and networks. This study believes that this review can pave the way for the development of improved machine-learning methods for classifying attacks in the IoMT environment.

Keywords: Medical Internet of Things, Healthcare systems, Machine Learning, Attack Classification

1. INTRODUCTION

The traditional healthcare systems are confronted with new problems as the number of patients continues to rise, and as accessibility to healthcare services becomes harder due to tight job schedules. To solve this problem and improve the healthcare domain's accuracy, reliability, performance, accessibility, and effectiveness, the Medical Internet of Things (MIoT) has evolved (Akhtar, Rahman, Sadia & Perwej, 2021). Medical Internet of Things is the group of devices connected to the Internet, to perform the processes and services that support healthcare (Wencheng, Zhiping, Yangyang, Fang, Shengqun, & Guoyan, 2018). It is equally regarded as a subset of the Internet of things. It includes medical devices, wearable sensors, and other equipment that are connected to the internet for data collection and analysis (Yazid,2023) Many Internet of Things (IoT) gadgets are compact, budget-friendly, and have insufficient computational capability and memory capacity to support the execution of current security software (Banu, Ahammed & Fathima, 2016). It is widely recognized that the vulnerability to cyber-attacks extends beyond just the IoMT devices; their associated data also face significant risks. The key importance of the IoMT system is to gather and transmit health information such as ECG, weight, blood pressure as well and sugar levels of patients.

The rapid evolution of IoMT has paved the way for the integration of medical devices and systems with the Internet. This integration has transformed healthcare by enabling real-time monitoring, remote patient care, and improved treatment outcomes. However, the increased connectivity and reliance on IoMT devices have brought about significant security challenges. Sadly, one of the

serious concerns about the IoMT framework revolves around privacy matters and potential data exposure (Gupta, Venugopal, Mahajan, Gaur, Barnwal & Mahajan, 2020b; Xu, Wei, Wang, Zhang & Zhou, 2020). The importance of ML techniques in IoMT security depends on the specific use case, available data, and the nature of attacks encountered in the IoMT environment. A balanced approach involving a combination of these ML techniques can provide a comprehensive and effective solution for classifying security attacks in IoMT systems. This study focuses on reporting the attack landscape as well as ML techniques for the classification of such attacks in the MIoT environment.

Wencheng *et al*. (2018) pointed out that those traditional security approaches, such as rule-based systems and signature-based detection, often struggle to keep up with the constantly evolving attack vectors and sophisticated techniques employed by malicious actors. The increasing complexity and interconnectedness of IoMT environments necessitate the use of advanced techniques to detect and classify attacks. Traditional security measures alone may not be sufficient to combat the evolving threat landscape in MIoT. Advanced MIoT attack classification techniques are needed because attacks are now sophisticated, and attack surfaces are fast growing. (Alsubaei, Abuhussein, & Shiva, 2019), as well as (He, Chan, Guizani, & Xu, 2018), have mentioned that researchers and security practitioners have turned to ML approaches to achieve improved attack detection. The authors further argued that ML techniques have shown promise in enhancing the security of IoMT devices by effectively classifying and detecting attacks in real time. This review aims to provide a comprehensive analysis of relevant literature on the applications of ML techniques for enhancing the security of IoMT devices.

This study aims to conduct a review of Machine Learning (ML) techniques that have been proposed for the classification of attacks in the IoMT environment. The specific objectives are to:

i. identify and source about Thirty-Five (35) relevant materials that focus on the utilisation of ML techniques for classifying attacks in IoMT environments; and
ii. review the recent and relevant literature sourced.

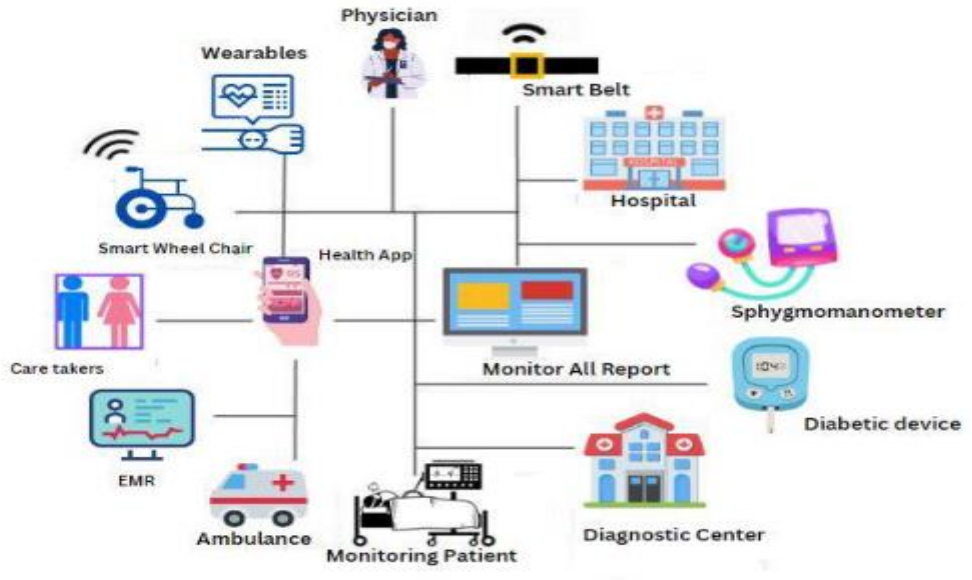

Figure 1: Internet of Medical Things (Yazid, 2023)

2. METHODOLOGY

The methodology used in this paper involves the stages itemized below. The various stages involve defining a search strategy, identifying study selection, and reporting the threat landscape in IoMT. Some of the notable research databases such as IEEE, Web of Science, Springer Link, Scopus, and Science Direct were used for the search. Subsequently, the most precise and applicable articles were isolated to address the research inquiries. Following that, the chosen papers underwent thorough scrutiny and examination. Ultimately, the review falls under conceptual and empirical studies.

2.1 Search Strategy

This study used the identified research repositories to source relevant literature that were published in English between the year 2016 and 2023. The searches were conducted using a wide range of search strings. The search phrases used were: "Machine learning techniques" AND "Attack detection in Medical Internet of Things " AND " Internet of Medical Things,", "Attacks in Health care systems" OR "Supervised Learning in Medical Internet of Things " OR "Predictive modeling approaches", "Medical Facility Security" AND "Cybersecurity threat detection in health care system" AND "Internet security". These search phrases were considered to obtain a good number of relevant studies in research repositories for the review being carried out. The researchers focused on studies or literature published in the English language and contained in journals (both printed and electronic), conference proceedings, and books between the years 2016 and 2023.

2.2 Study Selection Criteria

The objective of this stage is to refine the collection of papers obtained in the initial search, isolating studies with thematic relevance that could potentially address the primary research inquiries. The researcher established a set of criteria for inclusion and exclusion, alongside guidelines for evaluating the quality of the studies. The selection and refinement phases encompassed within this review are outlined as follows:

i. Use the predefined criteria for including and excluding papers.
ii. Eliminate any duplicated articles that are discovered across various databases.
iii. Utilize the quality assessment method to assign scores to the articles according to their relevance to the research questions.

Explore further related articles by referencing the sources cited in the articles acquired from Step 3, and subsequently reapply the assessment process as outlined in Step 3 to these additional articles.

Table 1: Predefined Inclusion and Exclusion Criteria

Criteria	Inclusion	Exclusion
Relevance	Studies focusing on the application of ML techniques for classifying attacks in IoMT.	Studies unrelated to IoMT security or attack classification.
Publication Type	Peer-reviewed journal articles, conference papers, technical reports, and dissertations.	Non-peer-reviewed sources, blogs, opinion pieces.
Time Frame	Studies published within the last 10 years (2016-2023), capture recent developments.	Studies published before 2016.
Methodology	Studies that employ ML techniques for attack classification in IoMT.	Studies focus solely on theoretical discussions without practical application.
Dataset	Studies using real-world or simulated datasets relevant to IoMT attack classification.	Studies without appropriate datasets or using irrelevant datasets.

Evaluation	Studies presenting a comprehensive evaluation of ML techniques' performance.	Studies lacking proper evaluation or performance metrics.
Comparison	Studies that compare and contrast different ML techniques for IoMT attack classification.	Studies do not provide comparative analysis.
Accessibility	Studies are accessible through available databases, repositories, conferences, and open-access sources.	Studies that are not accessible due to paywalls or limited availability.
Publication Status	Studies that are published or officially available.	Ongoing research, unpublished studies, or preprints.
Scope and Focus	Studies specifically address IoMT security and attack classification.	Studies that broadly discuss AI/ML or IoMT without a focus on attack classification.

3. ATTACK LANDSCAPE IN MEDICAL INTERNET OF THINGS

McGowan *et al*. (2021) defined the Internet of Things (IoT) as a system that uses the Internet to facilitate communication between sensors and devices. Thus, the Internet of Medical Things focuses on having a system that allows communication between sensors and devices that are tailored toward healthcare services. (Nayak *et al.,* 2022) pointed out that the vulnerabilities in IoMT devices allow unauthorized access for potential entry into healthcare and sensitive personal data.

With the advancement of modern technology, progressively ubiquitous medical devices raise critical security and data privacy concerns through resource constraints and open connectivity. Vulnerabilities in IoMT devices allow unauthorized access for potential entry into healthcare and sensitive personal data. Karmakar, Varadharajan, Tupakula, Nepal and Thapa, (2020) pointed out that the threat landscape refers to the entire scope of potential and recognized cybersecurity threats affecting user groups, and organizations. Hyder *et al*. (2021) equally emphasised that the attack landscape in the Internet of Things is generally growing. Attacks in the IoMT are of different types and can be achieved using different approaches. Examples of attacks include Unauthorized Access, Data Breaches, Malware and Ransomware, Denial of Service (DoS) Attacks, Man-in-the-Middle (MitM) Attacks, Device Manipulation, Physical Attacks, Insider Threats, Interoperability Issues, Lack of Security Updates and Social Engineering (He *et al.*, 2018),

Hameed *et al*. (2021) pointed out that there are attacks such as supply chain attacks, and regulatory and compliance challenges However, they can be classified using different ML approaches. For example, attackers use phishing tactics to illegally acquire private and sensitive data from unsuspecting online individuals. Some attackers launch denial-of-service attacks and man-in-the-middle attacks on healthcare facilities. To counteract the surge of cyberattacks rooted in phishing, various machine-learning methods have been suggested as more effective replacements for traditional signature-based methods (Oyelakin, 2021). The security of IoMT systems is very important due to the sensitive nature of the data involved, including personal health information and medical records. Therefore, ensuring the safety, uniqueness, and availability of this data is critical to maintaining patient privacy, protecting against potential breaches, and maintaining the trust of patients and healthcare providers. IoMT systems face a wide range of security threats and attacks.

McGowan, Sittig and Andel (2021) surveyed the threat and vulnerability landscape in the field of Medical Internet of Things. The study argued that the survey can be of great to other researchers in the field. Authors further mentioned that privacy and security vulnerabilities have appeared as challenges for IoT devices and they need to be adequately attended to. Specifically, attacks in the

IoMT can be classified as unauthorised access, data breaches, device tampering, denial-of-service attacks, as well as ransomware attacks (Fernandez, Huertas, Perales, Garcia, Weimer, & Lee, 2019).

4. MACHINE LEARNING

Machine Learning (ML) is defined as the field of study that gives computers the ability to learn without being explicitly programmed (Mahesh, 2020). It is used to teach machines how to handle data more efficiently. It is a subset of Artificial Intelligence (AI) that acquires knowledge and expertise through data and real-world encounters, all without the need for explicit programming (Kubat, 2017).

4.1 Machine Learning Techniques for the classification of attacks in IoMT

Machine learning techniques for the classification of attacks can be categorised as shallow and deep learning methods. In the shallow learning techniques, we have supervised unsupervised, and semi-supervised approaches. This study focuses on supervised learning which belongs to the shallow learning category as well as some Deep learning methods.

4.1.1 *Supervised Learning*

Supervised learning techniques are essential for classifying security attacks in MIoT due to their ability to learn from labeled training data. With labeled data, supervised learning algorithms, such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Naive Bayes classifiers, can effectively identify and distinguish attack patterns from normal behavior (Dridi, 2021). Supervised learning provides accurate and reliable results when sufficient labeled data is available for training.

4.1.2 *Deep Learning*

Deep learning techniques, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) hold significant importance in IoMT security. Deep learning models excel at learning complex patterns and hierarchical representations from raw data, making them well-suited for detecting sophisticated and previously unseen attack patterns (Mathew, Amudha & Sivakumar, 2021). With the abundance of data generated by IoMT devices, deep learning can be highly effective in identifying subtle and evolving attacks.

Usama, Qadir, Raza, Arif, Yau, Elkhatib and Al-Fuqaha (2019) pointed out that some examples of unsupervised learning techniques are: K-means clustering, DBSCAN, and Self-Organizing Maps (SOM) and they play a crucial role in IoMT security. They are used to detect anomalies in the absence of labeled data. It was argued that unsupervised learning is valuable when labeled attack data is scarce or when attacks are constantly evolving and not well-defined. These techniques are effective in detecting novel and zero-day attacks that may not be present in labeled datasets.

5. REVIEWED ARTICLES

Table 2: Summary of Reviewed Articles

Research Area	Author of the Study	Description
Deep Neural Network	Vijayakumar *et al. (*2023)	Introduced an advanced cyberattack detection system for IoMT using a Deep Neural Network. Specializes in multi-class classification, effectively identifying ARP Spoofing, DoS attacks, Nmap attacks, and Smurf attacks, achieving high true detection rates while minimizing false detections.
Machine Learning	Javed *et al. (*2023)	Conducted a comprehensive review of machine learning techniques addressing security concerns

Techniques for Security Control		in IoT, with a focus on security challenges in IoMT and IoV. Emphasized authentication, authorization, and data privacy in these sensitive domains.
Machine Learning for Cybersecurity in IoMT	Narang *et al.* (2022)	Conducted a thorough review of cybersecurity in IoMT, discussing various machine learning approaches and highlighting challenges and constraints in securing IoMT systems.
Optimized Deep Learning	Aruna & Vijaya (2021)	Proposed a machine learning-based attack detection model optimized for IoMT, demonstrating the potential of deep learning techniques in IoMT security.
LSTM-Based Detection	Nayak *et al. (*2022) & Li *et al.* (2021)	Nayak et al. presented a machine learning-based model for enhanced decision-making accuracy in IoMT. Li et al. introduced a two-phase LSTM-based method for detecting network protocols and IoT anomalies in healthcare, addressing imbalanced data.
Intrusion Detection System (IDS)	Saheed & Arowolo (2021)	Explored the utilization of deep recurrent neural networks (DRNN) and supervised machine learning models to build a robust intrusion detection system in IoMT.
Deep Belief Network (DBN)	Manimurugan *et al.(*2021)	Introduced a Deep Belief Network (DBN) algorithm for intrusion detection in IoMT, achieving impressive accuracy across various attack categories.
Machine Learning Applications in Healthcare	McGowan *et al*. (2021)	Emphasized the potential of machine learning for attack classification within the IoMT domain, specifically in healthcare settings.
General IoT and Ransomware	Cui *et al.*, (2018) & Sgandurra *et al.* 2016)	Cui et al. conducted a comprehensive survey of machine learning applications in the broader IoT domain. Sgandurra et al. proposed the machine learning-based method "EldeRan" for dynamically analyzing and classifying ransomware activities, enhancing IoT security.
IoMT Security and Privacy	Sun, Lo, & Lo (2019), Newaz *et al*., (2020), and Yaacoub et al. (2020)	Sun, Lo, & Lo reviewed IoMT security and privacy, focusing on authentication and access control. Newaz et al. conducted a survey addressing security and privacy threats in healthcare systems within IoMT. Yaacoub et al. reviewed security issues and limitations in IoMT, emphasizing lightweight security solutions.

These studies collectively showcase the growing importance of machine learning techniques in enhancing security and privacy within IoMT and IoT domains, addressing various challenges and paving the way for improved healthcare and patient data protection.

6. MACHINE LEARNING (ML) TECHNIQUES AND THEIR STRENGTHS

Some of the strengths of ML approaches are as follows:

i. Powerful Pattern Recognition: ML techniques, especially deep learning models, are highly effective at recognizing complex and subtle attack patterns from vast amounts of data generated in IoMT healthcare services.
ii. Scalability: ML models can efficiently handle large datasets and scale to accommodate the growing number of IoMT devices and the volume of data they produce.
iii. Wide Applicability: ML techniques offer a broad range of algorithms suitable for different IoMT attack classification scenarios, providing flexibility in implementation.
iv. Transfer Learning: ML models can leverage pre-trained models or knowledge from other domains, potentially enhancing the detection of new attacks in IoMT healthcare.

6.1 Limitations of ML Techniques and Recommended Solutions

i. Data Requirements: ML techniques, especially deep learning, often demand a large amount of labeled data for training, which can be challenging to obtain in IoMT healthcare settings due to privacy concerns and data scarcity. Combine a small amount of labeled data with a larger pool of unlabeled data and leverage semi-supervised learning techniques to maximize the use of available data. Utilize transfer learning by fine-tuning pre-trained models on your specific IoMT security dataset, reducing the need for extensive labeled data. Apply data augmentation techniques to synthetically increase the size of the dataset and improve model robustness.
ii. Overfitting: ML models, if not carefully designed and regularized, can suffer from overfitting, leading to reduced generalization and erroneous predictions. Meanwhile, cross-validation to assess model performance and tune hyperparameters to prevent overfitting can be implemented. It is also good to utilize regularization techniques like L1 and L2 regularization to penalize complex models and promote generalization
iii. Interpretability: Some ML models, especially complex deep learning architectures, lack interpretability, making it difficult to understand the reasoning behind their classifications, which is critical in healthcare decision-making. It is recommended to create visualizations of model decisions and feature importance to enhance the understanding of IoMT security alerts and predictions. Also, it is good to utilize model-agnostic interpretability techniques like SHAP values, LIME, or feature importance analysis to gain insights into black-box models.
iv. Resource Intensiveness: Training and deploying sophisticated ML models may require substantial computational resources, which could be a limitation for resource-constrained IoMT devices. However, it is better to implement edge computing to offload some security processing tasks from IoMT devices to more powerful edge servers, reducing the resource burden. Also, using lightweight cryptographic algorithms specifically designed for resource-constrained devices to secure data transmission and storage efficiently will go a long way.

7. DISCUSSIONS

The study reported that ML techniques are generally powerful and promising in security. Several relevant pieces of literature were sourced and adequately reviewed to understand the current trends in the use of ML approaches for IoMT attack classification. Specifically, these techniques can handle large-scale and diverse data more efficiently and can identify patterns in the security domain. This study further found out that ML techniques can have significant impacts such as early detection, data privacy, anomaly detection, adaptive security, and resource optimization on both healthcare security and patient safety. However, it is essential to be mindful of ethical considerations such as Privacy Preservation, Bias and Fairness, Informed Consent, and Data Security; and also stay informed about emerging trends and challenges like Explainable AI, Robustness against Adversarial Attacks, Real-time Monitoring, Secure Federated Learning, Standardization and Cyber Insurance

8. CONCLUSION

This paper focuses on review of articles in the area of classification of attacks in Internet of Medical of Things. The study grouped some of the sources searched and reviewed them under different headings. This review emphasized the various attacks in IoMT as well as the key concepts in the field of using machine learning techniques for classifying the attacks. The review has highlighted the diverse strengths inherent in ML techniques. This study further mentioned that ML models can learn to identify and classify attacks in IoMT and then achieve a higher degree of accuracy and speed. The adaptability and resilience exhibited by ML techniques, especially deep learning models, demonstrate exceptional capability in discerning intricate patterns from expansive datasets as it is a vital trait in a domain characterized by abundant data. The synthesis of existing literature underscores that these techniques, whether in isolation or synergy, offer multifaceted solutions to the intricate security challenges synonymous with IoMT healthcare services. It is believed the paper can serve as insights for other researchers who want to work in this domain.

REFERENCES

[1] Akhtar, N., Rahman, S., Sadia, H., &Perwej, Y. (2021). A Holistic Analysis of Medical Internet of Things (MIoT), *Journal of Information and Computational Science*, 11(4), 209-222.

[2] Alsubaei F, Abuhussein A, Shiva S. 2019a. A framework for ranking IoMT solutions based on measuring security and privacy. In: Arai K, Bhatia R, Kapoor S, eds. *Proceedings of the Future.*

[3] Aruna Santhi, J. & Vijaya Saradhi, T. (2021).Attack detection in medical Internet of Things using optimized deep learning: enhanced security in healthcare sector, Data Technologies and Applications, Vol. 55 No. 5, pp. 682-714. https://doi.org/10.1108/DTA-10-2020-0239

[4] Banu, R., Ahammed, G.F.A., Fathima, N., (2016). A review of biologically inspired approaches to security for the Internetof Things (IoT). In: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1062–1066,ttps://doi.org/10.1109/ICEEOT.2016.7754848

[5] Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., & Qin, J. (2018). A survey on application of machine learning for Internet of Things. *International Journal of Machine Learning and Cybernetics*, *9*, 1399-1417.

[6] Dridi, S. (2021). Supervised learning-a systematic literature review. *preprint, Dec*.

[7] Fernandez Maimo, L., Huertas Celdran, A., Perales Gomez, A. L., Garcia Clemente, F. J., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors*, *19*(5), 1114.

[8] Gupta, K. D., & Dagsputa, D. (2021). Negative selection algorithm research and applications in the last decade: A review. *IEEE Transactions on Artificial Intelligence*, *3*(2), 110-128.

[9] Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science*, *7*, e414.

[10] He D, Ye R, Chan S, Guizani M, Xu Y. 2018. Privacy in the Internet of things for smart healthcare. *IEEE Communications Magazine 56(4):38–44 DOI* 10.1109/MCOM.2018.1700809

[11] Hussain F, Hussain R, Hassan SA, Hossain E. 2020. Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials 22(3):1686–1721.

[12] Javed A, Awais M, Shoaib M, Khurshid KS, Othman M. 2023. Machine learning and deep learning approaches in IoT. Peer J Computer Science 9:e1204 https://doi.org/10.7717/peerj-cs.1204

[13] Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y., & Moussa, S. (2023). Internet of Medical Things privacy and security: Challenges, solutions, and future trends from a new perspective. *Sustainability*, *15*(4), 3317.

[14] Karmakar K. K., Varadharajan V., Tupakula U., Nepal S. & Thapa C. (2020).Towards a security-enhanced virtualized network infrastructure for the internet of medical things (iomt), in 6th IEEE Conference on Network Softwarization (NetSoft), 257–261, IEEE, 2020.

[15] Krishna Kant Singh, Mohamed Elhoseny, Ahmed A. Elngar (2021).Machine Learning and the Internet of Medical Things in Healthcare, Science Direct Books and Journals, DOI https://doi.org/10.1016/C2019-0-03077-4

[16] Kubat, M., & Kubat, M. (2017). Induction in multi-label domains. *An introduction to machine learning*, 251-271.

[17] Li-ChuWu, Chia-Mei Chen, Zheng-Xun Cai, Ming Hsia Hsu, Wang-Chuan Juang(2021).Machine Learning-Based Detection of Internet of Thing Attacks in Healthcare Environments, retrieved from https://www.it-iindustry.com/issue/archive/117.html

[18] Mahesh, B. (2020). Machine learning algorithms a review. *International Journal of Science and Research (IJSR) [Internet]*, *9*(1), 381-386.

[19] Manimurugan S., Al-Mutairi Saad , Aborokbah Majed Mohammed, Chilamkurti Naveen ,Ganesan Subramaniam & Patan Rizwan (2021).Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network, Special Section On Deep Learning Algorithms for Internet of Medical Things Retrieved From Https://Ieeexplore.Ieee.Org/Ielx7/6287639/8948470/09057709.Pdf

[20] Mathew, A., Amudha, P., &Sivakumari, S. (2021). Deep learning techniques: an overview. *Advanced Machine Learning Technologies and Applications: Proceedings of MLTA 2020*, 599-608.

[21] McGowan Aleise, Sittig Scott M, Andel Todd R. (2021). Medical Internet of Things: A Survey of the Current Threat and Vulnerability Landscape, DOI: 10.24251/HICSS.2021.466, Conference: Hawaii International Conference on System Sciences (HICSS)

[22] Hyder Muhammad Faraz et al. (2021).Attack Detection in IoT using Machine Learning, Engineering, Technology and Applied Science Research 11(3):7273-7278, DOI: 10.48084/etasr.4202

[23] Narang, Mohita and Jatain, Aman and Punetha, Nirmal (2022). A study on Cyber-attack detection in IoMT using Machine Learning Techniques, *Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022*, Available at SSRN: https://ssrn.com/abstract=4387775 or http://dx.doi.org/10.2139/ssrn.4387775

[24] Nayak, J., Meher, S.K., Souri , A. *et al.* (2022).Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *Journal Super Comput* 78, 14866–14891. https://doi.org/10.1007/s11227-022-04453-z

[25] Newaz A, Sikder AK, Rahman MA, Uluagac AS. 2020. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. Available htttps://arxiv.org/abs/2005.07359.

[26] Oyelakin, A. M. (2021). An investigation into the performances of supervised Learning algorithms in different phishing datasets. *Pakistan Journal of Engineering, Technology & Science*, *9*(2).

[27] Perwej, Y. (2015). An Evaluation of Deep Learning Miniature Concerning Soft Computing. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(2), 10-16.

[28] Saheed Yakub Kayode & Arowolo Micheal Olaolu (2021). Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning

Algorithms, images, retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9617609 16th September 2023

[29] Sgandurra, L. Muñoz-González, Mohsen R., and Lupu E. C., "Automated Dynamic Analysis of Ransomware: Benefits, Limitations, and Use for Detection," 2016, [Online]. Available: http://arxiv.org/abs/1609.03020.

[30] Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. *Future generation computer systems*, *78*, 956-963.

[31] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ...& Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications, and research challenges. *IEEE Access*, *7*, *65579-65615*.

[32] Vijayakumar, Kedalu Poornachary, Krishnadoss Pradeep, Ananthakrishnan Balasundaram, and Manas Ranjan Prusty (2023). Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network, *Processes*, 1072. https://doi.org/10.3390/pr11041072, 2023, *11*(4), 1072; https://doi.org/10.3390/pr11041072.

[33] Wencheng Sun, ZhipingCai, Yangyang Li, Fang Liu, Shengqun Fang, and Guoyan Wang (2018). Security and Privacy in the Medical Internet of Things: A Review, Security and Communication Networks, 2018, DOI: 10.1155/2018/5978636.

[34] Xu J, Wei L, Wu W, Wang A, Zhang Y, Zhou F. 2020. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical systems. Future Generation Computer Systems 108(1):1287–1296 DOI10.1016/j.future.2018.04.018.Technologies, Conference. Cham: Springer International Publishing Ag, 205–224.

[35] Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A. (2020).Securing internet of medical things systems: limitations, issues, and recommendations. Future Generation Computer Systems, 105(10):581–606 DOI10.1016/j.future.2019.12.028.

[36] Yazid, A. (2023). Cybersecurity and Privacy Issues in the Internet of Medical Things (IoMT). *Eigenpub Review of Science and Technology*, *7*(1), 1-21, https://studies.eigenpub.com/index.php/erst

Author's Brief Profile

Olomu J. O. is currently a master's student in the Department of Computer Science at Al-Hikmah University, Ilorin, Nigeria. He holds a Postgraduate Diploma in Computer Science from the University of Ilorin, Ilorin, Nigeria; and he's currently a [4]Postgraduate Researcher at, the Department of Computer Science, Al-Hikmah University, Ilorin, Nigeria, Nigeria. His research areas include Machine Learning, Cybersecurity, and Computational Sciences. He is happily married with kids. He can be reached by phone through e-mail at luability4u@gmail.com

Oyelakin A. M. (Ph.D., MNCS) received his National Diploma (ND) and First Degree in Computer Science from Federal Polytechnic, Offa, and the University of Ilorin respectively. He finished with Distinction and Second Class Upper respectively. He had his Master's in Computer Science from the University of Lagos, Akoka in 2014. He also obtained PhD in Computer Science from the University of Ilorin, Ilorin, Nigeria in 2021. Before joining academia on a full-time basis, he worked in different capacities as IT personnel in Information Technology, Oil Servicing, and Aviation. He has published more than thirty-five papers in refereed journals and conference proceedings. His areas of research interest include Data and Computer Networks, Security/Privacy, Mobile Computing, Machine Learning, and Medical Image Segmentation. He is a member of the Nigeria Computer Science and Internet Society. He is happily married with kids.

Ayinla O. M. (MNCS) is currently a master's student in the Department of Computer Science at Al-Hikmah University, Ilorin, Nigeria. He received a Bachelor's degree in Mathematics and Computer Science from the National Open University of Nigeria (NOUN). Currently a Postgraduate Researcher at, the Department of Computer Science at Al-Hikmah University, Nigeria. His research areas include Machine Learning, Cybersecurity, and Computational Sciences. He is happily married with kids. He can be reached at ayinlamutiu2019@gmail.com.

Ibrahim H. A. is currently a master's student in the Department of Computer Science at Al-Hikmah University, Ilorin, Nigeria. She holds a First Degree in Computer Science and Engineering from Ladoke Akintola University, Ogbomoso, Nigeria. She graduated with Second Class Upper in 2011. Her area of research interest is Cyber Security. She is happily married with kids. She can be reached via: igehabiba@gmail.com