JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(3), SEPTEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

An Intrusion Detection System for the Internet of Medical Things (IoMT): An Artificial Intelligence (AI) Approach

Emmanuel Araba, Paul Moggridge
Department of Computer Science,
University of Hertfordshire, UK

ABSTRACT

The Internet of Medical Things (IoMT) is a network of linked medical devices, including pacemakers, prosthetic limbs, glucometers, smartwatches, and more, integrated with software programs and healthcare infrastructure. IoMT has transformed healthcare by solving long-standing problems, but because of its design, it raises questions about the security and privacy of patient information. Finding reliable solutions to protect IoMT network traffic is vital because using older systems can disclose weaknesses and attract potential cyber threats. Intrusion detection systems (IDS) have recently become a key component of IoMT network security. Machine learning (ML) systems have demonstrated impressive efficacy in intrusion detection over the past few decades. Nevertheless, research examining the potential of ML algorithms for IDS in IoMT networks needs to be more comprehensive. In this regard, this research delves into the intricate realm of network traffic threat analysis, employing the CICDDoS2019 dataset encompassing 44,687 rows and 88 diverse columns. Through meticulous data preprocessing, missing values were addressed, and redundant columns were pruned, leading to a refined dataset of 62 columns. Post-data transformation and normalisation, machine learning implementations, specifically XGBoost and Random Forest algorithms, were employed for classification tasks. The initial XGBoost model showcased an accuracy of 97.62%, which, after hyperparameter optimisation, slightly rose to 97.71%. Concurrently, the Random Forest Classifier demonstrated an initial accuracy of 96.65%, which increased to 97.64% post-optimisation. Both models exhibited robust classification capabilities across varied network traffic types, with exceptional performance in classifying "BENIGN" traffic. The study underscores the pivotal role of hyperparameter tuning in enhancing machine learning model performance and presents insights into the nuanced classification of network traffic threat in the IoMT environment.

ARTICLE INFO
Article History
Received: July, 2023
Received in revised form: July, 2023
Accepted: September, 2023
Published online: September, 2023

KEYWORDS
Machine learning, Intrusion detection system (IDS), Internet of Medical Things

INTRODUCTION

COVID-19 pandemic has placed numerous countries in a dire situation, presenting a significant risk to human life due to increased social interaction (Fontanet et al., 2021). The difficult circumstance of the pandemic necessitates technical innovation to deliver effective healthcare services to isolated patients and prevent the spread of infection. Similarly, the Internet of Medical Things (IoMT) is anticipated as a viable option to help doctors maintain social distancing and provide remote treatment, which is necessary to address the current pandemic crisis (Siddiqui, 2021). The rapid progress in IoT technology has expedited the adoption of IoMT and paved the way for developing intelligent healthcare systems and more efficient healthcare services for patients. Several nations have implemented IoMT to facilitate timely diagnosis through continuous patient monitoring in real-time and to save lives during the unpredictable crisis of pandemics (Udgata et al., 2021).

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

IoMT, or Healthcare IoT, refers to integrating various healthcare devices and information technology systems to facilitate the sharing sensitive patient data with medical professionals, enabling personalised medical responses. IoMT has introduced new possibilities in healthcare, providing patients with the convenience of receiving quality medical services from the comfort of their homes. Additionally, it can reduce costs by minimising unnecessary hospital visits and stays (Lu, Qi and Fu, 2019). In addition to significant improvements in the precision of diagnosis and accuracy of treatment, IoMT offers many benefits. According to Siddiqui (2021), healthcare providers see IoMT as a cornerstone for addressing the pandemic crisis by remotely monitoring and treating multiple patients simultaneously without requiring additional healthcare facilities.

Enabling Wireless Technologies and IoMT

Internet of Things (IoTs) networks are made up of sensors and devices connected by cloud ecosystems and made possible by high-speed connectivity between each part. These sensors and devices quickly communicate the raw data they have collected to the vast storage space offered by cloud services. This data is then cleaned up and analysed for more profound implications. Additional software, tools, and programs that support the visualisation, analysis, processing, and general data management are required to complete this task.

The many wireless technologies shown in Figure 1 include RFID (Radio Frequency Identification), NFC (Near Field Communications), Bluetooth, LTE (Long Term Evolution), and more recent versions like 5G/6G and beyond. A wide variety of products, including smartphones, monitoring equipment, sensors, wearable technology, and other medical devices, are connected through these wireless technologies. The Internet of Medical Things (IoMT) is widely adopting 5G/6G and future iterations, principally because of its large bandwidth and deficient latency characteristics.

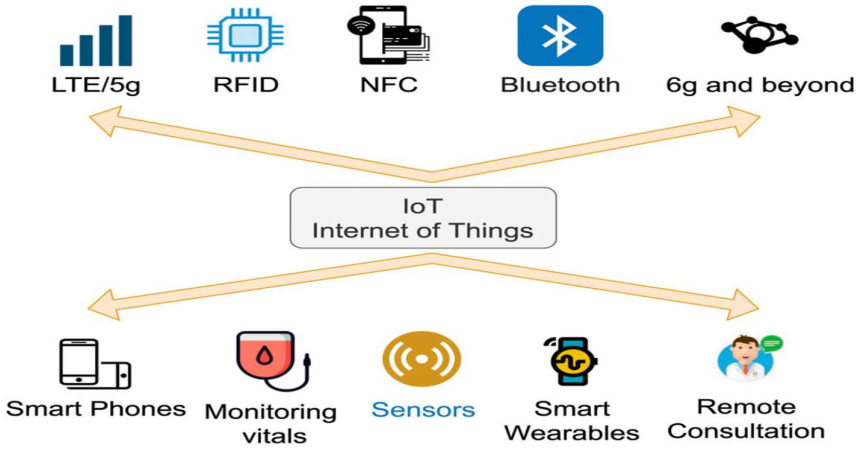

Figure 1: Devices and enabling technologies for the IoTs (Razdan and Sharma, 2022)

Statement of Problem

The Internet of Medical Things (IoMT) ecosystem is still vulnerable to a variety of new cyber risks and assaults because of its open nature and broad use, despite its many benefits (Asif et al., 2021; Hatzivasilis et al., 2019). Cybercriminals interested in using increasingly sophisticated cyberattacks to take advantage of its shortcomings have been drawn to it due to its open nature and susceptible design. These gadgets are a good target for different threat actors that can engage in abnormal behaviors against them because to their extensive connectivity and ongoing data sharing (Moradi, Moradkhani and Tavakoli, 2022). Cyberattacks on IoMT could have devastating effects and endanger the lives of patients (Alqaralleh et al., 2021).

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

IoMT devices weakness have been further emphasized by recent investigations. According to an analysis of actual Internet of Things (IoT) devices, firmware has a number of security flaws and hazards, including risky operations, exploitable vulnerabilities, and additional attack surfaces. Another extensive empirical investigation revealed that 28.25 percent of IoT devices had at least one N-days vulnerability, highlighting the grave dangers that these flaws present (Zhao et al., 2020). In addition, a sizable proportion of consumer IoT devices are susceptible to attacks that could jeopardize user privacy and information (Williams et al., 2017).

According to research, IoMT devices have significant security vulnerabilities that must be fixed in order to prevent hostile cyberattacks (Rahman and Jahankhani, 2021). In general, IoMT systems are prone to a variety of threats, and many security measures are insufficient to protect them. However, it has been demonstrated that the majority of known threats may be mitigated by proposed security frameworks (Ghubaish et al., 2020).

In summary, IoMT security has developed into a critical problem of global concern that has to be addressed right now in order to ensure its successful implementation and continued expansion in the years to come.

Objectives of the Study

This study aims to build an Artificial Intelligence (AI)-driven intrusion detection system (IDS) to address increasing cyber threats in the Internet of Medical Things (IoMT) environments. The objectives of the research are to:

1. The usage of machine learning algorithms has been presented to enable an intelligent framework to detect threats quickly and effectively in the IoMT environment.
2. Employ a publicly available, state-of-the-art CICDDoS2019 dataset to evaluate the performance of the proposed model.
3. Evaluate the proposed model's performance by employing selected existing benchmark algorithms.
4. Utilise standard evaluation metrics for proper assessment.
5. Conduct a comprehensive evaluation of the proposed model's performance.

Research Questions

The researcher's research questions in the study focus on the following:

1. Do the standard evaluation metrics employed in the study accurately assess the proposed model's performance in detecting and mitigating cyber threats?
2. Through a comprehensive evaluation and comparative analysis, do the machine learning models improve after hyperparameter tuning?

LITERATURE REVIEW

In this literature review, the Internet of Medical Things (IoMT) is explored in a number of different ways. The use of deep convolutional neural networks for the diagnosis of COVID-19 and ML algorithms for detecting brain cancers and monitoring cardiovascular disorders are just two examples of how AI and machine learning are being applied in the e-health domains. Application of AI/ML for E-health domains is highlighted in Section 2.1. The implementation of Software-Defined Networking (SDN) in IoMT is highlighted in Section 2.2 with examples including identifying botnets and optimizing network resources for e-healthcare services. Section 2.3 focuses on the integration of AI tools in Intrusion Detection Systems (IDS) for IoMT, emphasizing deep learning-based IDS and their potential to enhance security. The review concludes in Section 2.4, summarizing key findings and underlining the transformative potential of AI/ML and SDN in healthcare delivery, diagnostics, and security, while also acknowledging challenges like the opacity of AI techniques and the need for tailored solutions in IoMT.

Related Works

The linked works covered in this literature review shed light on significant developments in the Internet of Medical Things (IoMT) setting in the areas of healthcare, networking, and security. These studies provide fundamental building blocks for comprehending the complex IoMT technology landscape. They include cutting-edge uses of AI and ML in

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

healthcare, the incorporation of Software-Defined Networking (SDN) for network administration, and the creation of effective Intrusion Detection Systems (IDS) adapted to the particular difficulties of IoMT. In the age of connected medical devices and data, these research collectively contribute to the continuous revolution of healthcare delivery, diagnosis, and cybersecurity.

Application of AI/ML for E-health Domains.

According to Lalmuanawma, Hussain and Chhakchhuak (2020), techniques from machine learning (ML) and artificial intelligence (AI) have been used to improve the diagnosis and screening processes for people with COVID-19. This improvement is made possible using "radio imaging" technology based on the same principles as well-established techniques like computed tomography (CT), X-ray imaging, and data processing from blood samples.

The integration of AI and ML solutions goes to improving network security and privacy. This is demonstrated in Abdelkefi, Jiang and Sharma (2018) study, which introduces an AI/ML-based method for the identification of Distributed Denial of Service (DDoS) assaults as well as specific privacy violations.

Application SDN in IoMT in providing Slicing and Network Management.

Liaqat et al. (2020) describe the deployment of an AI-driven software-defined networking (SDN) solution to recognise botnets with malevolent intent. Furthermore, Cecil et al. (2018) introduce a novel SDN-based method for surgical training in the Internet of Medical Things (IoMT) context. Various telehealth applications, such as telemedicine, telesurgery, and surgical planning, demonstrate the value of this paradigm. In addition, Askari et al. (2021) present an SDN-based scheduling strategy for Non-Orthogonal Multiple Access (NOMA) systems. This method considers things like latency, energy expenditure, and channel conditions. The results show considerable throughput, network latency, and energy efficiency gains.

Artificial Intelligence (AI) Tools in Intrusion Detection Systems of IoMT

Idrissi, Azizi and Moussaoui (2020) conducted a study that emphasised the security threats and vulnerabilities associated with IoT. Their primary focus was on Deep Learning-based Intrusion Detection Systems. The findings from their research can serve as a roadmap for future research directions, particularly in IoT security with deep learning methodologies. Their study underscores the potential of deep learning in enhancing the robustness of intrusion detection systems in IoT environments.

Binbusayyis et al. (2022) aimed to fill the knowledge gap by investigating the application of various machine learning (ML) algorithms for intrusion detection in IoMT networks. Binbusayyis et al. (2022) study analysed the performance of K-nearest neighbor, Naïve Bayes, support vector machine, artificial neural network, and decision tree algorithms. The analysis results provided valuable insights into the effectiveness of these ML approaches for building efficient intrusion detection systems to protect IoMT networks against malicious activities.

RESEARCH DESIGN

The suggested intrusion detection system (IDS) in the context of the Internet of Medical Things (IoMT) is the study design's focus, presenting a quantitative approach to answering the research objectives. It involves gathering actual data, combining pertinent literature, and using current methods for benchmarking. A complete preparation step includes cleaning and normalisation of the data. For their strength in classification, XGBoost and Random Forest are two important machine learning algorithms. A model stacking strategy incorporating both techniques improves the IDS performance. Standard metrics are used in performance evaluation to assess how well the system detects cyber threats. The research design ensures that the methodology is organised and systematic, directing the investigative process. Figure 3 shows the proposed framework for the study below.

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(3), SEPTEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

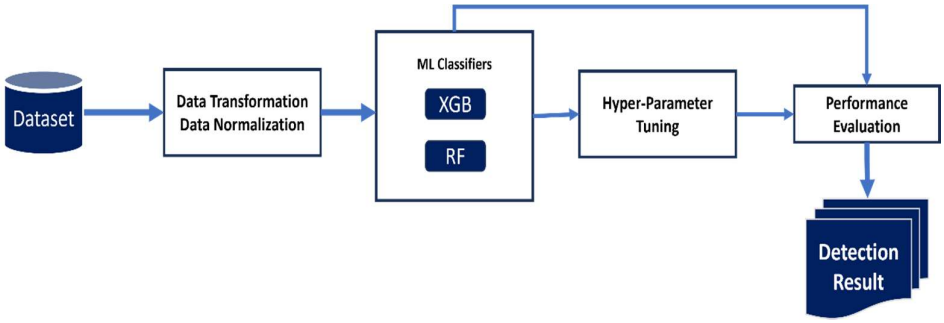

Figure 3.: Proposed Framework for AI-based IDS

Data Normalisation: Assuring proportional contribution and eliminating bias toward features with higher values in ML algorithms, normalisation is standardising all features' values to a uniform scale. This work uses Z-score normalisation (Binbusayyis and Vaiyapuri, 2019) as described in Eq. (1), acknowledging its importance in data preparation for increased predictive capability. This technique scales all features in the [0,1] range while taking the mean (μ) and standard deviation (σ) into consideration. The Python library performs this scaling function as the RobustScaler.

$$x^* = \frac{x-\mu}{\sigma} \quad (1)$$

IDS Machine Learning Techniques

The main goal of the analytical study is to assess and compare the effectiveness of several machine learning algorithms for spotting intrusions in IoMT networks. Below is a brief description of each of the two different ML algorithms covered by this inquiry.

XGBClassifier

An implementation of the gradient boosted decision trees technique created for speed and performance is called XGBClassifier. Gradient boosting is an ensemble learning technique that develops weak learners sequentially, usually decision trees. Each branch fixes the mistakes made by its forerunner. "Extreme Gradient Boosting" or "XGBoost" is particularly well-known since it performs well in various machine learning competitions. The main idea of XGBoost is to employ the gradient descent technique to reduce loss while including new models. The algorithm's target objective function for XGBoost is denoted by Eq. (2):

$$Obj(\theta) = \sum_i^n l(y_i, \hat{y}_i) + \sum_i^n \Omega(f_i) \quad (2)$$

Where:
L is the training loss function.
y_i is the true label for the i-th instance.
$\hat{y}_i$ is the predicted label for the i-th instance.
Ω represents the regularisation term to prevent overfitting.
f_i is the model's prediction for the i-th instance.

The regularisation term Ω in XGBoost is given by Eq. (3):

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda \sum_{j=1}^{T} w_j^2 \quad (3)$$

Where:
T is the number of leaves in the tree.
w_j is the score assigned to the j-th leaf.
γ and λ are regularisation parameters.

The effectiveness of XGBClassifier was highlighted in a study by Monika, Kumar and Kumar (2021), who showed that when they experimented with different feature detectors and descriptors, XGBClassifier outperformed other classifiers in terms of accuracy, precision, recall, F1-score, and area under the curve.

ENVIRONMENT/EXPERIMENTAL SETUP

The controlled setting created to carry out the study's experiments and assessments is described in this chapter. It details the essential elements, materials, equipment, and assessment criteria included in the experimental framework for in-depth study.

Evaluation metrics of IDS for IoMT

When evaluating and contrasting the performance of a proposed IDS versus currently used techniques, it is crucial to have a solid awareness of the standardised measures used

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

within the IDS development and research community. Many metrics or criteria must be used to assess an IDS's efficacy in the context of IoMT. These metrics include.

Detection Related Metrics

The classifier needs to undergo training using the training data from the IDS dataset and subsequently be tested using the testing data from the same CICIDDoS2019 dataset. The outcomes of an IDS evaluation can be categorised as follows:

1. True Positive (TP) refers to the amount of malicious material that has been accurately discovered, classified as suspicious, and is present in IoMT network traffic.
2. True Negative (TN) signifies the volume of benign data within the IoMT network traffic, correctly identified and categorised as expectedly benign.
3. False Positive (FP) refers to the benign or normal instances within IoMT network traffic that are inaccurately classified as malicious samples or attacks.
4. False Negative (FN) corresponds to malicious samples within the IoMT network traffic mistakenly classified as normal instances.

Confusion Matrix

The Confusion Matrix is a technique for describing the thorough output of a specific categorisation model. By incorporating four important metrics—False Negative (FN), False Positive (FP), True Negative (TN), and True Positive (TP)—it provides a comprehensive perspective of the categorisation effectiveness (Sohn, 2021). Figuring this out is Figure 4.

		Actual: Positive	Actual: Negative
Predicted	Positive	True Positive	False Positive
	Negative	False Negative	True Negative

Figure 4: Confusion Matrix

Sensitivity, recall, precision, F1 score, and accuracy are other significant measures to assess IDS performance. The evaluation metrics based on the confusion matrix are presented below (Rbah et al., 2022).

1. **Accuracy:** This is the percentage of accurate forecasts out of all the predictions. Eq. (4) shows the mathematical representation:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (4)$$

2. **Precision:** A statistic for determining how well a machine learning model predicts the total number of true positives out of all anticipated positives. Eq. (5) shows the mathematical representation:

$$Precision = \frac{TP}{TP+FN} \quad (5)$$

3. **Recall/Sensitivity:** A metric for assessing the ML model's precision in counting the total number of true positives compared to all false positives. Eq. (6) shows the mathematical representation:

$$Recall = \frac{TP}{TP+FP} \quad (6)$$

4. **Specificity:** The percentage of actual negative events projected to be negative. Eq. (7) shows the mathematical representation:

$$\text{Specificity} = \frac{TN}{FP+TN} \quad (7)$$

5. **F-1 Score (Measure):** A harmonic average of the recall and precision metrics to assess the model's performance. Eq. (8) shows the mathematical representation:

$$F1-score = 2 * \left(\frac{(Precision \times Recall)}{(Precision + Recall)}\right) (8)$$

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(3), SEPTEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

6. **False Positive Rate (FPR):** The percentage of negative samples that were incorrectly classified compared to all other negative cases. Eq. (9) shows the mathematical representation:

$$\text{FPR} = \frac{FP}{FP+TN} \quad (9)$$

7. **False Negative Rate (FNR):** It measures the ratio of incorrectly identified positive samples to all positive samples. Eq. (10) shows the mathematical representation:

$$\text{FNR} = \frac{FN}{TP+FN} \quad (10)$$

EXPERIMENTAL SETUP

On the online Google Colab portal, a Python notebook was used to carry out all the experiments described in this study. All of the classifiers used in this work were implemented using Python and the Scikit-learn package, which offers a wide range of cutting-edge machine learning techniques. The Pandas, NumPy, SciPy, and matplotlib libraries are the backbone of Scikit-learn's capability. This combination yields a simple yet effective data mining and analysis tool.

The CICIDDoS2019 dataset was divided into many sets in order to handle it. A cross-validation approach optimised the model using an 80 percent fraction as the training set. The testing set, which comprised the remaining 80%, was crucial in evaluating the model and recording the testing results.

RESULT DISCUSSION, PROJECT MANAGEMENT AND RELEVANCE

Dataset

The dataset has 88 columns and 44,687 rows, and it contains a variety of data kinds, including 34 columns are int64-type, 49 are float64-type, and 5 are classified as objects. The Flow Bytes/s column has 2 missing values, and the rows affected were removed, giving a complete dataset for analysis. The "Label" column in the dataset classifies different kinds of network traffic and lists the instances of each category. In particular, "Portmap" was noticed 9,960 times, followed by "LDAP" (9,931), "NetBIOS" (9,785), "MSSQL" (9,658), and "BENIGN" (5,353). In contrast to the other listed special protocols, the designation "BENIGN" denotes cases determined to be benign or non-malicious.. Figure 5 shows the plot of the distribution.

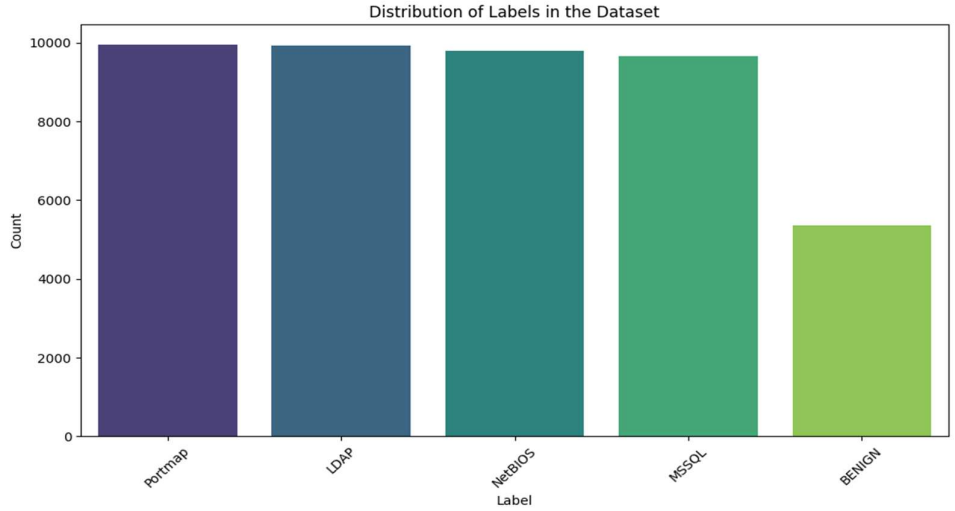

Figure 5: Distribution of Labels

Data Transformation and Normalisation

Firstly, the "Label" column in the transformed dataset, representing various network traffic threats, has been encoded to facilitate computational processing. The mapping is "BENIGN" to 0, "LDAP" to 1, "MSSQL" to 2, "NetBIOS" to 3, and "Portmap" to 4, respectively. The beginning rows in the

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

revised dataset now include both the original "Label" and its corresponding encoded counterpart under the "Label_encoded" column, offering a clear point of reference for analysis and modelling.

Before running the scaler and normalisation, it was encountered that the dataset contains values that are either infinity or too large for the float64 data type. The columns (Flow Bytes/s and Flow Packets/s) were identified and dropped.

Machine Learning Implementation

First, the dataset was divided into training and testing sets using the train-test-split library, following an 80-20 ratio. The dataset consists of two parts: the training set (X_train) with 35,749 samples, each having 54 features, and the testing set (X_test) with 8,938 samples, also each characterised by 54 features. Following this preprocessing step, both the XGBoost and Random Forest algorithms were implemented.

Table 1: Optimisation of the hyperparameters for ML algorithms

ML Models	Parameter	Values	Optimal Value
XGBoost	learning_rate	0.01, 0.1	0.1
	n_estimators	100, 500	100
	max_depth	3, 6, 9	6
	Subsample	0.5, 0.9	0.9
	colsample_bytree	0.5, 0.9	0.5
Random Forest	n_estimators	100, 300, 500	300
	max_depth	None, 10, 20, 30	20
	min_samples_split	2, 5, 10	10
	min_samples_leaf	1, 2, 4	1

Hyperparameter-tuned XGBoost

The XGBoost model's overall accuracy increases somewhat after applying hyperparameter adjustment, going from 97.62% to 97.71%. The 'LDAP' precision, in particular, has perfected itself at 1.00. While 'Portmap' witnessed an increase in precision from 0.96 to 0.97, 'NetBIOS' recall increased from 0.96 to 0.97. Even if these enhancements seem insignificant, they can greatly impact real-world situations, supporting the advantages of hyperparameter adjustment for model optimisation. Table 4 shows the classification representation of the hyper-tuned XGBoost algorithm.

Table 2: Hyperparameter evaluation of XGBoost

Label	Precision	Recall	F1-Score	Support
BENIGN	1	1	1	1071
LDAP	1	0.99	0.99	1986
MSSQL	1	0.99	1	1932
NetBIOS	0.94	0.97	0.95	1957
Portmap	0.97	0.94	0.95	1992

In the confusion matrix for the hyperparameter-tuned XGBoost model, 'BENIGN' traffic was impeccably classified, with all 1,071 instances correctly identified. 'LDAP' saw 1,973 accurate classifications out of 1,986, with minor diversions to 'MSSQL' and 'Portmap'. 'MSSQL' garnered 1,913 correct predictions from 1,932, with slight misclassifications towards 'LDAP' and 'Portmap' and a solitary instance as 'BENIGN'. Of its 1,957 instances, 1,854 were accurately tagged for' NetBIOS', but 103 were misdirected to 'Portmap'. Lastly, 'Portmap' achieved 1,828 correct classifications out of 1,992, with most errors leaning towards 'NetBIOS'. Figure 9 shows the confusion matrix of the hyper-tuned model.

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(3), SEPTEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

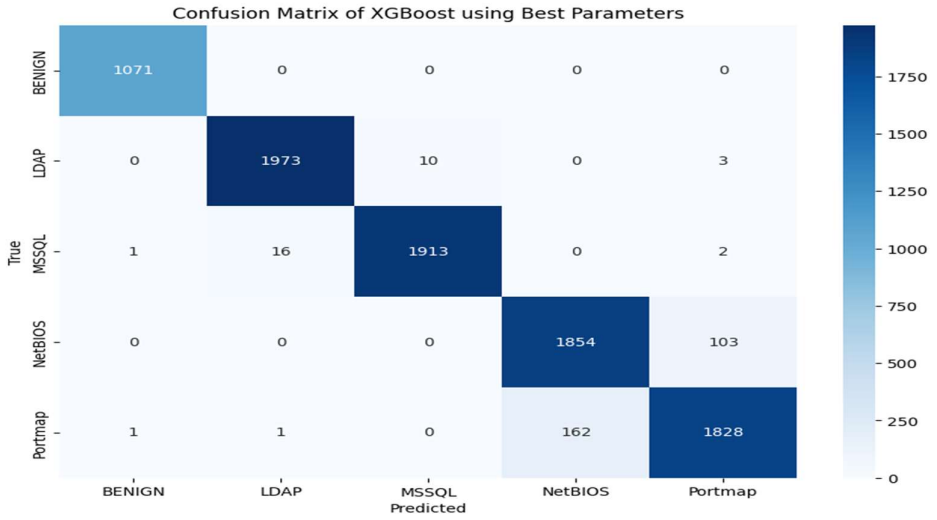

Figure 9: Confusion matrix of XGBoost using the best parameters.

Hyperparameter-tuned Random Forest

The Random Forest Classifier's accuracy increased somewhat after hyperparameter adjustment, rising from 96.65% to 97.64%. A careful analysis of each category shows that the precision for "NetBIOS" and "Portmap" improved, going to 0.95 and 0.96, respectively. The improvement in 'NetBIOS' and 'Portmap' precision underlines the refinement by hyperparameter optimisation, leading to a more robust and finely-tuned model than the initial Random Forest implementation. While categories like 'BENIGN', 'LDAP', and 'MSSQL' maintained their high-performance metrics. Table 5 shows the classification report of the hyper-tuned model.

Table 3: Classification Report of Tuned Random Forest model

Label	Precision	Recall	F1-Score	Support
BENIGN	1	1	1	1071
LDAP	0.99	0.99	0.99	1986
MSSQL	1	0.99	0.99	1932
NetBIOS	0.95	0.96	0.96	1957
Portmap	0.96	0.94	0.95	1992

According to the confusion matrix, the hyperparameter-tuned Random Forest model has outstanding classification abilities. All 1,071 occurrences of "BENIGN" traffic's classification were perfectly accurate. 1,974 of the 1,986 instances of 'LDAP' were correctly tagged, with only minor errors of 'MSSQL' (7 instances) and 'Portmap' (5 instances) occurring. The 'MSSQL' category had a success rate of 1,915 correct predictions out of 1,932, with a few 'LDAP' and 'Portmap' forecasts slightly off. Out of 1,957 occurrences, 'NetBIOS' correctly classified 1,885 while misclassifying 72 others as 'Portmap'. Last but not least, "Portmap" classified 1,882 correctly out of 1,992 instances, with a few incorrect classifications primarily affecting "NetBIOS." Figure 10 shows the confusion matrix for the hyperparameter-tuned Random Forest model.

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

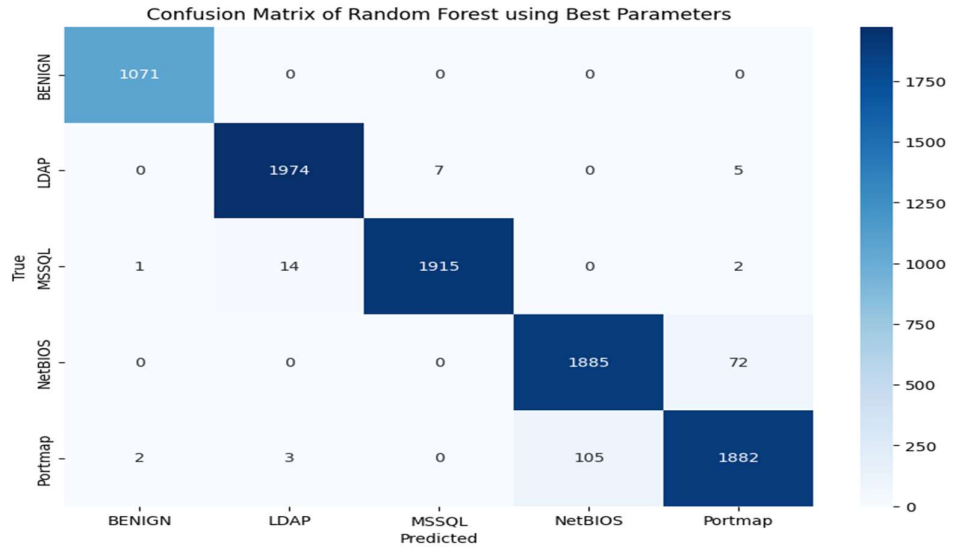

Figure 10: Confusion Matrix of Random Forest using Best Parameters.

Commercial and Economic Context of the Research

1. From a business standpoint, implementing a cutting-edge AI-based IDS fills a crucial gap for enterprises in delicate and exposed industries like healthcare. Developing networked medical devices and data-sharing platforms in the IoMT offers thieves rich chances to exploit flaws. This research gives enterprises a useful way to reduce security risks by providing a new, intelligent framework for quick and efficient threat detection. Commercial entities, including healthcare organisations and medical device makers, can adopt and integrate this system to strengthen their security measures and safeguard sensitive patient data, intellectual property, and operational continuity.
2. Economically, the research supports the expansion of the cybersecurity industry, which is witnessing exploding demand on a global scale. The market for AI-driven cybersecurity solutions is growing quickly as businesses invest in cutting-edge technologies to protect their operations. The creative IDS may tap this market suggested in this study, opening up new commercialisation and income generation opportunities. The results of this study can be used by startups, well-established cybersecurity companies, and global technology leaders to create, promote, and sell cutting-edge intrusion detection products specifically designed for IoMT environments. The ensuing economic activity can foster innovation, generate jobs, and aid in expanding the technology sector.

RESEARCH FINDINGS

This research delves into and comprehensively analyses two distinct machine learning algorithms (XGBoost and Random Forest) used for intrusion detection. The study examined the CICIDDoS2019 dataset with 88 columns (features) and 44687 rows (instances) containing different forms of data. After data pre-processing, the dataset was reduced to 62 columns, which included handling missing values and deleting superfluous columns based on high correlation. The "Label" column, symbolising various network traffic threats, was encoded to speed up computer processing. With "Portmap" having the highest

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

representation and "BENIGN" having the lowest.

Using the Google Colaboratory environment, the dataset was used to implement the XGBoost and Random Forest machine learning algorithms. On the test dataset, the XGBoost model initially displayed an impressive accuracy of 97.62%. When the hyperparameters were adjusted, its accuracy merely increased to 97.71%. In contrast, the Random Forest Classifier started with an accuracy of 96.65% and rose to 97.64% after hyperparameter adjustment. The precision of categories like "NetBIOS" and "Portmap" showed a noticeable increase following optimisation, highlighting the importance of hyperparameter adjustment in improving the model's performance.

The thorough confusion matrices for both algorithms demonstrate how well they can classify various types of network data. The capacity of both models to identify between different forms of network traffic was strong, with "BENIGN" traffic being practically perfectly categorised in both situations. Both algorithms were strong, but the hyperparameter-tuned versions performed better, demonstrating the value of careful parameter tuning in machine learning models for obtaining the best outcomes.

Conclusion

The conclusions derived from this study highlight how important it is to choose the best ML algorithm for IDS in IoMT networks and pave the way for further development in this area. The IoMT ecosystem's risks are ever more complicated and nuanced as it continues to develop. Recommendations

This study offers a crucial baseline for those exploring ML-based IDS and a clear path for future research. Researchers can better adapt their strategies to solve the particular difficulties presented by IoMT networks by analysing the benefits and drawbacks of current ML algorithms in detecting intrusions.

In the future, there are plans to delve further into the complexity of both traditional ML and cutting-edge deep learning methods. In the context of IoMT, the objective is to assess each's efficacy, adaptability, and scalability. Due to the fundamental nature of many IoMT applications, from industrial automation to healthcare, security is essential.

Additionally, more than just conducting the theoretical study is required. Moving from theoretical models to practical applications is equally important. Therefore, support for the active implementation and thorough testing of these algorithms in real IoMT devices is essential. A hands-on approach provides vital input that enables incremental improvements and guarantees that the IDS solutions work in theory and practice.

REFERENCES

Abdel-Basset, M., Hawash, H., Chakrabortty, R.K. and Ryan, M.J. (2021) 'Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks', *IEEE Internet of Things Journal*, 8(15) IEEE, pp. 12251–12265.

Abdelkefi, A., Jiang, Y. and Sharma, S. (2018) 'SENATUS: an approach to joint traffic anomaly detection and root cause analysis', *2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, pp. 1–8.

Ahmad, R. and Alsmadi, I. (2021) 'Machine learning approaches to IoT security: A systematic literature review', *Internet of Things*, 14 Elsevier, p. 100365.

Ahmed, Z., Mohamed, K., Zeeshan, S. and Dong, X. (2020) 'Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine', *Database*, 2020 Oxford University Press, p. baaa010.

Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I. and Guizani, M. (2020) 'A survey of machine and deep learning methods for internet of things (IoT) security', *IEEE Communications Surveys & Tutorials*, 22(3) IEEE, pp. 1646–1685.

Alqaralleh, B.A.Y., Vaiyapuri, T., Parvathy, V.S., Gupta, D., Khanna, A. and Shankar, K. (2021) 'Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment', *Personal and Ubiquitous Computing* Available at:

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

10.1007/s00779-021-01543-2 (Accessed: 21 April 2023).

Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X. (2017) 'Fog computing for the internet of things: Security and privacy issues', *IEEE Internet Computing*, 21(2) IEEE, pp. 34–42.

Alsubaei, F., Abuhussein, A. and Shiva, S. (2019) 'A framework for ranking IoMT solutions based on measuring security and privacy', *Proceedings of the Future Technologies Conference (FTC) 2018: Volume 1*. Springer, pp. 205–224.

Aman, A.H.M., Hassan, W.H., Sameen, S., Attarbashi, Z.S., Alizadeh, M. and Latiff, L.A. (2021) 'IoMT amid COVID-19 pandemic: Application, architecture, technology, and security', *Journal of Network and Computer Applications*, 174 Elsevier, p. 102886.

Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W. and Wahab, A. (2020) 'A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions', *Electronics*, 9(7) MDPI, p. 1177.

Asif, M., Khan, W.U., Afzal, H.R., Nebhen, J., Ullah, I., Rehman, A.U. and Kaabar, M.K. (2021) 'Reduced-complexity LDPC decoding for next-generation IoT networks', *Wireless Communications and Mobile Computing*, 2021 Hindawi Limited, pp. 1–10.

Askari, Z., Abouei, J., Jaseemuddin, M. and Anpalagan, A. (2021) 'Energy-efficient and real-time NOMA scheduling in IoMT-based three-tier WBANs', *IEEE Internet of Things Journal*, 8(18) IEEE, pp. 13975–13990.

Badotra, S., Nagpal, D., Panda, S.N., Tanwar, S. and Bajaj, S. (2020) 'IoT-enabled healthcare network with SDN', *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, pp. 38–42.

Bagci, I.E., Raza, S., Roedig, U. and Voigt, T. (2016) 'Fusion: coalesced confidential storage and communication framework for the IoT', *Security and Communication Networks*, 9(15) Wiley Online Library, pp. 2656–2673.

Benadda, B., Beldjilali, B., Mankouri, A. and Taleb, O. (2018) 'Secure IoT solution for wearable health care applications, case study Electric Imp development platform', *International Journal of Communication Systems*, 31(5) Wiley Online Library, p. e3499.

Binbusayyis, A., Alaskar, H., Vaiyapuri, T. and Dinesh, M. (2022) 'An investigation and comparison of machine learning approaches for intrusion detection in IoMT network', *The Journal of Supercomputing*, 78(15), pp. 17403–17422.

Binbusayyis, A. and Vaiyapuri, T. (2019) 'Identifying and benchmarking key features for cyber intrusion detection: An ensemble approach', *IEEE Access*, 7 IEEE, pp. 106495–106513.

Biswas, R. and Roy, S. (2021) 'Botnet traffic identification using neural networks', *Multimedia Tools and Applications*, 80 Springer, pp. 24147–24171.

Boutaba, R., Salahuddin, M.A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F. and Caicedo, O.M. (2018) 'A comprehensive survey on machine learning for networking: evolution, applications and research opportunities', *Journal of Internet Services and Applications*, 9(1) Springer, pp. 1–99.

Butun, I., Morgera, S.D. and Sankar, R. (2013) 'A survey of intrusion detection systems in wireless sensor networks', *IEEE communications surveys & tutorials*, 16(1) IEEE, pp. 266–282.

Cecil, J., Gupta, A., Pirela-Cruz, M. and Ramanathan, P. (2018) 'An IoMT based cyber training framework for orthopedic surgery using Next Generation Internet technologies', *Informatics in Medicine Unlocked*, 12 Elsevier, pp. 128–137.

Deogirikar, J. and Vidhate, A. (2017) 'Security attacks in IoT: A survey', *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, pp. 32–37.

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

Divekar, A., Parekh, M., Savla, V., Mishra, R. and Shirole, M. (2018) 'Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives', *2018 IEEE 3rd international conference on computing, communication and security (ICCCS)*. IEEE, pp. 1–8.

Dominguez, R. (2007) 'Denial of service attack', *The Blackwell Encyclopedia of Sociology*, Wiley Online Library, pp. 1–1.

Dutta, M. and Granjal, J. (2020) 'Towards a secure Internet of Things: A comprehensive study of second line defense mechanisms', *IEEE Access*, 8 IEEE, pp. 127272–127312.

Esfahani, A., Mantas, G., Silva, H., Rodriguez, J. and Neves, J.C. (2016) 'An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems', *EURASIP Journal on Wireless Communications and Networking*, 2016(1) SpringerOpen, pp. 1–10.

Esfahani, A., Mantas, G., Yang, D., Nascimento, A., Rodriguez, J. and Neves, J. (2015) 'Towards secure network coding-enabled wireless sensor networks in cyber-physical systems', *Cyber-Physical Systems: From Theory to Practice*, CRC Press, pp. 395–414.

Fontanet, A., Autran, B., Lina, B., Kieny, M.P., Karim, S.S.A. and Sridhar, D. (2021) 'SARS-CoV-2 variants and ending the COVID-19 pandemic', *The Lancet*, 397(10278) Elsevier, pp. 952–954.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G. and Vázquez, E. (2009) 'Anomaly-based network intrusion detection: Techniques, systems and challenges', *computers & security*, 28(1–2) Elsevier, pp. 18–28.

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A. and Jain, R. (2020) 'Recent advances in the internet-of-medical-things (IoMT) systems security', *IEEE Internet of Things Journal*, 8(11) IEEE, pp. 8707–8718.

Hajar, M.S., Al-Kadri, M.O. and Kalutarage, H.K. (2021) 'A survey on wireless body area networks: Architecture, security challenges and research opportunities', *Computers & Security*, 104 Elsevier, p. 102211.

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G. and Tsatsoulis, C. (2019) 'Review of security and privacy for the Internet of Medical Things (IoMT)', *2019 15th international conference on distributed computing in sensor systems (DCOSS)*. IEEE, pp. 457–464.

Hindy, H., Brosset, D., Bayne, E., Seeam, A.K., Tachtatzis, C., Atkinson, R. and Bellekens, X. (2020) 'A taxonomy of network threats and the effect of current datasets on intrusion detection systems', *IEEE Access*, 8 IEEE, pp. 104650–104675.

Hommersom, A., Lucas, P.J., Velikova, M., Dal, G., Bastos, J., Rodriguez, J., Germs, M. and Schwietert, H. (2013) 'MoSHCA-my mobile and smart health care assistant', *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*. IEEE, pp. 188–192.

Hu, J., Yu, X., Qiu, D. and Chen, H.-H. (2009) 'A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection', *IEEE network*, 23(1) IEEE, pp. 42–47.

Huang, C.-H., Lee, T.-H., Chang, L., Lin, J.-R. and Horng, G. (2019) 'Adversarial Attacks on SDN-Based Deep Learning IDS System', *Mobile and Wireless Technology 2018*. Springer, Singapore, pp. 181–191. Available at: 10.1007/978-981-13-1059-1_17 (Accessed: 21 April 2023).

Idrissi, I., Azizi, M. and Moussaoui, O. (2020) 'IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review', *2020 Fourth international conference on intelligent computing in data sciences (ICDS)*. IEEE, pp. 1–10.

Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M. and Kwak, K.-S. (2015) 'The internet of things for health care: a comprehensive

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

survey', *IEEE access*, 3 IEEE, pp. 678–708.

Javeed, D., Badamasi, U.M., Iqbal, T., Umar, A. and Ndubuisi, C.O. (2020) 'Threat detection using machine/deep learning in IOT environments', *International Journal of Computer Networks and Communications Security*, 8(8) Dorma Trading, Est. Publishing Manager, pp. 59–65.

Khan, S.R., Sikandar, M., Almogren, A., Din, I.U., Guerrieri, A. and Fortino, G. (2020) 'IoMT-based computational approach for detecting brain tumor', *Future Generation Computer Systems*, 109 Elsevier, pp. 360–367.

Khorshidpour, Z., Hashemi, S. and Hamzeh, A. (2017) 'Evaluation of random forest classifier in security domain', *Applied Intelligence*, 47(2), pp. 558–569.

Kilic, A. (2020) 'Artificial intelligence and machine learning in cardiovascular health care', *The Annals of thoracic surgery*, 109(5) Elsevier, pp. 1323–1329.

Kissel, R. (2011) *Glossary of key information security terms*. Diane Publishing.

Kumar, P., Gupta, G.P. and Tripathi, R. (2021) 'An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks', *Computer Communications*, 166 Elsevier, pp. 110–124.

Lalmuanawma, S., Hussain, J. and Chhakchhuak, L. (2020) 'Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: A review', *Chaos, Solitons & Fractals*, 139 Elsevier, p. 110059.

Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X. and Gong, L. (2018) 'Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN', *International Journal of Communication Systems*, 31(5) Wiley Online Library, p. e3497.

Li, J., Zhao, Z., Li, R. and Zhang, H. (2019) 'AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks', *IEEE Internet of Things Journal*, 6(2), pp. 2093–2102.

Liaqat, S., Akhunzada, A., Shaikh, F.S., Giannetsos, A. and Jan, M.A. (2020) 'SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)', *Computer Communications*, 160 Elsevier, pp. 697–705.

Lu, Y., Qi, Y. and Fu, X. (2019) 'A framework for intelligent analysis of digital cardiotocographic signals from IoMT-based foetal monitoring', *Future Generation Computer Systems*, 101, pp. 1130–1141.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P. and Ni, W. (2018) 'Anatomy of threats to the internet of things', *IEEE communications surveys & tutorials*, 21(2) IEEE, pp. 1636–1675.

Mebawondu, J.O., Alowolodu, O.D., Mebawondu, J.O. and Adetunmbi, A.O. (2020) 'Network intrusion detection system using supervised learning paradigm', *Scientific African*, 9 Elsevier, p. e00497.

Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A. (2018) *Handbook of applied cryptography*. CRC press.

Modi, C.N. and Acha, K. (2017) 'Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review', *the Journal of Supercomputing*, 73(3) Springer, pp. 1192–1234.

Monika, Kumar, M. and Kumar, M. (2021) 'XGBoost: 2D-object recognition using shape descriptors and extreme gradient boosting classifier', *Computational Methods and Data Engineering: Proceedings of ICMDE 2020, Volume 1*. Springer, pp. 207–222.

Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., Virtanen, S., Tenhunen, H. and Isoaho, J. (2016) 'End-to-end security scheme for mobility enabled healthcare Internet of Things', *Future Generation Computer Systems*, 64 Elsevier, pp. 108–124.

Moradi, M., Moradkhani, M. and Tavakoli, M.B. (2022) 'Security-level improvement of IoT-based systems using biometric features', *Wireless Communications*

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

and Mobile Computing, 2022 Hindawi Limited, pp. 1–15.

Morgenstern, J.D., Rosella, L.C., Daley, M.J., Goel, V., Schünemann, H.J. and Piggott, T. (2021) '"AI's gonna have an impact on everything in society, so it has to have an impact on public health": a fundamental qualitative descriptive study of the implications of artificial intelligence for public health', *BMC Public Health*, 21(1), p. 40.

Moustafa, N. and Slay, J. (2016) 'The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set', *Information Security Journal: A Global Perspective*, 25(1–3) Taylor & Francis, pp. 18–31.

Nieles, M., Dempsey, K. and Pillitteri, V.Y. (2017) 'An introduction to information security', *NIST special publication*, 800(12), p. 101.

Organization, W.H. (2018) 'What do we mean by availability, accessibility, acceptability and quality (AAAQ) of the health workforce', *Global Health Workforce alliance, World Health Organization. retrieved from http://www. who. int/workforcealliance/media/qa/04/en*

Özgür, A. and Erdem, H. (2016) '*A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015*', PeerJ Preprints

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J. and Lymberopoulos, D. (2022) 'A survey on security threats and countermeasures in internet of medical things (IoMT)', *Transactions on Emerging Telecommunications Technologies*, 33(6) Wiley Online Library, p. e4049.

Razdan, S. and Sharma, S. (2022) 'Internet of medical things (IoMT): Overview, emerging technologies, and case studies', *IETE technical review*, 39(4) Taylor & Francis, pp. 775–788.

Rbah, Y., Mahfoudi, M., Balboul, Y., Fattah, M., Mazer, S., Elbekkali, M. and Bernoussi, B. (2022) 'Machine learning and deep learning methods for intrusion detection systems in iomt: A survey', *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*. IEEE, pp. 1–9.

Rodrigues, J.J., Segundo, D.B.D.R., Junqueira, H.A., Sabino, M.H., Prince, R.M., Al-Muhtadi, J. and De Albuquerque, V.H.C. (2018) 'Enabling technologies for the internet of health things', *Ieee Access*, 6 IEEE, pp. 13129–13141.

Sætra, H.S. (2021) 'A Framework for Evaluating and Disclosing the ESG Related Impacts of AI with the SDGs', *Sustainability*, 13(15) Multidisciplinary Digital Publishing Institute, p. 8503.

Scholl, M.A., Stine, K., Hash, J., Bowen, P., Johnson, L.A., Smith, C.D. and Steinberg, D. (2008) '*An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule*', Matthew A. Scholl, Kevin Stine, Joan Hash, Pauline Bowen, L A. Johnson …

Sedik, A., Hammad, M., Abd El-Samie, F.E., Gupta, B.B. and Abd El-Latif, A.A. (2021) 'Efficient deep learning approach for augmented detection of Coronavirus disease', *Neural Computing and Applications*, Springer, pp. 1–18.

Sethi, K., Madhav, Y.V., Kumar, R. and Bera, P. (2021) 'Attention based multi-agent intrusion detection systems using reinforcement learning', *Journal of Information Security and Applications*, 61 Elsevier, p. 102923.

Shafiq, M., Tian, Z., Sun, Y., Du, X. and Guizani, M. (2020) 'Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city', *Future Generation Computer Systems*, 107 Elsevier, pp. 433–442.

Sharma, S., Nag, A., Cordeiro, L., Ayoub, O., Tornatore, M. and Nekovee, M. (2020) 'Towards explainable artificial intelligence for network function virtualization', *Proceedings of the 16th*

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK

International Conference on Emerging Networking Experiments and Technologies., pp. 558–559.

Shirey, R. (2007) *Internet security glossary, version 2*.

Siddiqui, M.F. (2021) 'IoMT Potential Impact in COVID-19: Combating a Pandemic with Innovation', in Raza, K. (ed.) *Computational Intelligence Methods in COVID-19: Surveillance, Prevention, Prediction and Diagnosis*. Studies in Computational Intelligence. Singapore: Springer, pp. 349–361. Available at: 10.1007/978-981-15-8534-0_18 (Accessed: 21 April 2023).

Sohn, I. (2021) 'Deep belief network based intrusion detection techniques: A survey', *Expert Systems with Applications*, 167, p. 114170.

Song, H., Bai, J., Yi, Y., Wu, J. and Liu, L. (2020) 'Artificial intelligence enabled Internet of Things: Network architecture and spectrum access', *IEEE Computational Intelligence Magazine*, 15(1) IEEE, pp. 44–51.

Thomas, C., Sharma, V. and Balakrishnan, N. (2008) 'Usefulness of DARPA dataset for intrusion detection system evaluation', *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008*. SPIE, Vol.6973, pp. 164–171.

Turabieh, H., Salem, A.A. and Abu-El-Rub, N. (2018) 'Dynamic L-RNN recovery of missing data in IoMT applications', *Future Generation Computer Systems*, 89 Elsevier, pp. 575–583.

Wahab, O.A. (2022) 'Intrusion detection in the iot under data and concept drifts: Online deep learning approach', *IEEE Internet of Things Journal*, 9(20) IEEE, pp. 19706–19716.

Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W. and Camtepe, S. (2021) 'Ae-mlp: A hybrid deep learning approach for ddos detection and classification', *IEEE Access*, 9 IEEE, pp. 146810–146821.

Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A. and Gulliver, S.R. (2020) 'Artificial intelligence for cybersecurity: a systematic mapping of literature', *IEEE Access*, 8 IEEE, pp. 146598–146612.

Williams, R., McMahon, E., Samtani, S., Patton, M. and Chen, H. (2017) 'Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach', *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, pp. 179–181.

Wu, J., Guo, S., Li, J. and Zeng, D. (2016) 'Big data meet green challenges: Greening big data', *IEEE Systems Journal*, 10(3) IEEE, pp. 873–887.

Yaacoub, J.-P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A. (2020) 'Securing internet of medical things systems: Limitations, issues and recommendations', *Future Generation Computer Systems*, 105 Elsevier, pp. 581–606.

Zhao, B., Ji, S., Lee, W.-H., Lin, C., Weng, H., Wu, J., Zhou, P., Fang, L. and Beyah, R. (2020) 'A large-scale empirical study on the vulnerability of deployed IoT devices', *IEEE Transactions on Dependable and Secure Computing*, 19(3) IEEE, pp. 1826–1840.

Corresponding author: Emmanuel, Araba
ea.araba@outlook.com
Department of Computer Science, University of Hertfordshire, UK