Received 18 August 2024, accepted 6 September 2024, date of publication 13 September 2024, date of current version 24 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3460428

RESEARCH ARTICLE

Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management

OLUWASEUN PRISCILLA OLAWALE[1] **AND SAHAR EBADINEZHAD**[1,2]

[1]Department of Computer Information Systems, Near East University, 99138 Nicosia, Cyprus
[2]Computer Information Systems Research and Technology Center (CISRTC), Near East University, 99138 Nicosia, Cyprus

Corresponding author: Sahar Ebadinezhad (sahar.ebadinezhad@neu.edu.tr)

ABSTRACT The Internet of Healthcare Things (IoHT) is an emerging critical technology for managing patients' health. They are prone to cybersecurity vulnerabilities because they are connected to the internet, primarily by wireless connections. This is a major concern, considering data privacy and security. Artificial intelligence (AI) models are excellent methods to detect and mitigate cybersecurity vulnerabilities. Since medical Information Technology (IT) is evolving and data privacy is a major concern with sensors generally, in healthcare IoT. The TON_IOT, Edge_IIoT, and UNSW-NB15 datasets were used in this study for assessment and implementation to solve the challenge using the chosen benchmark AI models with the integration of IPFS blockchain technology in order to decentralize and secure the data. Justifiable parameters were used to determine how efficient each technique is in predicting the best outcome. The results show the efficiency of the utilized models, particularly the Support Vector Machines (SVM). The TON_IoT dataset obtained 100% accuracy, the Edge_IIoT dataset obtained 98% accuracy, and the UNSW-NB15 dataset obtained 89% accuracy. The integrated blockchain technology in this model is applied for security purposes. Utilizing these techniques will proffer a secure and safe transmission of medical data. This study will generally provide important insight to other researchers in the healthcare field.

INDEX TERMS Artificial intelligence, abnormal behavior, healthcare, intrusion detection systems, IoT.

I. INTRODUCTION

Concerns about cybersecurity and patient privacy have arisen as a result of the IoHT systems' increasing connectivity and data interchange. Blockchain technology (BCT) is a recent advancement that brings about utmost data security and integrity, as well as trust in IoHT settings. It is well known for its immutable and decentralized nature. There are a lot of positives when this technology is considered, including unique safe authentication, information security, and enforced access control for mitigating current cybersecurity issues in IoHT. BCT ensures that patient data is securely encrypted to prevent intruders from gaining access to such information [1], as seen in Fig. 1. The logic structure of BCT, which is executed in smart contracts, enacts access control as an extra layer of security for IoHT settings. The build-up of a blockchain comprises a series of blocks structured to protect and verify information, thereby establishing trust among parties involved. This has led numerous researchers to make findings about this technology in particular [2].

IoHT is the case study in this research; hence, BCT will be used to enhance the security aspect, while AI will be used for most simulation processes. Also, BCT will be used to validate the AI models. Therefore, by integrating BCT into this work, processes will enable IoHT data points to trust each other while securing the blocks. Cybersecurity issues in IoHT arise due to improper architectural values, as well as a lack of regulations and standards [3]. Hence, there is a need to study the integration of AI and blockchain to decentralize and secure the data. A distinct confidentiality problem with IoHT systems is users consenting to the providers' agreement policy on data. BCT can be used to resolve such issues, according

The associate editor coordinating the review of this manuscript and approving it for publication was Mueen Uddin.

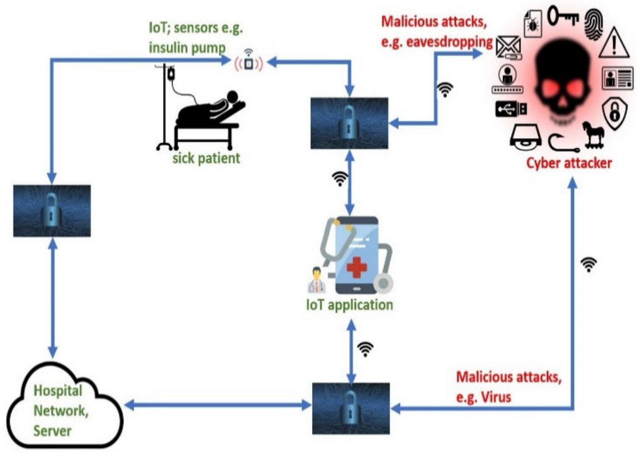

IoT; sensors e.g. insulin pump
sick patient
Malicious attacks, e.g. eavesdropping
Cyber attacker
IoT application
Malicious attacks, e.g. Virus
Hospital Network, Server

FIGURE 1. Blockchain security for IoHT.

to Elangovan et al. [4]. Implementing BCT means that centralized servers will be completely ruled out. This may pose a difficult situation because a centralized server is one of the main architectures of IoHT. BCT supports the continual flow of current data while simultaneously boosting the overall security and privacy of IoT devices through methodical validation of each transaction and network request. AI cannot be left out, as it assists network personnel in monitoring networks (wired or wireless) and detecting cyber intrusions.

This brings about an impressive system, with parties having records of transactions each time a transaction is made to the blockchain. Healthcare is a domain where blockchain technology shows tremendous promise, owing to its proclivity towards a patient-centric paradigm within the healthcare system. Researchers are making great efforts to implement BCT with Electronic Health Records (EHRs) [4].

The use of centralized servers poses a challenge to data authentication and transmission, preventing the security and privacy of data. These centralized servers are vulnerable due to Single Points of Failure (SPOF), false system permissions, and privacy issues. It does not cover the security and privacy of IoHT needs. To resolve this, a decentralized InterPlanetary File System (IPFS-blockchain system) has been implemented in this study. The IPFS supports privacy by generating a reference point termed content identifier [5]. Abnormal activities such as erroneous authentication, device spoofing, and decreased data exchange dependability are challenges that may be present. Kumara and Mallick [6] proposed a system to mitigate these issues. BCT was combined with the IoT architecture. This technique attempts to promote the security and privacy features of IoT by employing two main characteristics of BCT. BCT has brought about at a positive impact on the proceeds and outcomes of healthcare entities, ensuring optimization of business processes, efficient management of patient data, enhancement of patient outcomes, cost reduction, reinforcement of compliance, and improved utilization of healthcare-related data. This can also help to solve the risks associated with counterfeit drugs, ultimately protecting patients [2].

Machine learning (ML) is very present in almost every piece of technology. That is to say, complicated systems cannot do without them these days. While ML has improved life generally, it is primarily important in healthcare to identify sickness trends and mutations, potentially speeding up medication development. AI and ML can deliver health monitoring and consultation services using health bots. AI and IoHT can create analytic representations from data, monitor vital signs, and prevent cybercriminals from gaining access to confidential IoHT data [7]. Also, AI and ML assist medical personnel in the decision-making of patient cases [8]. The selected AI models used in this study were chosen based on their strengths from the work of other researchers [9]. Furthermore, the use of some of the models in the healthcare domain for cybersecurity anomaly detection is scarce in the literature. CNN and SVM were mentioned in our previous work [7]. Since these models have obtained reasonable results, they have the potential to greatly improve IoHT security.

Blockchain, cybersecurity, and AI are an integral part of the current advancements in technology. A blockchain implementation creates a secure framework that makes use of cryptography [10] for data storage and exchange, protecting the integrity and transparency of digital transactions. Simultaneously, cybersecurity procedures serve a critical role in protecting data from potential hostile activity [11]. Zubaydi et al. [12] highlighted several works addressing the combined use of BCT and IoHT to resolve several elements of privacy and security. Following that, applications were classified according to the initial parameters, objectives, development levels, target applications, types of blockchain and platforms used, consensus algorithms used, assessment settings and parameters, and any pending works or open problems. The authors presented an extensive Systematic Literature Review (SLR); however, there is no particular guide for the actual implementation of AI integration with IPFS-BCT in the healthcare domain in the literature. This research may serve as a guide for that purpose. The contribution of our research to the existing body of knowledge are:

1) Detection malicious activities (in terms of cybersecurity) that may cause IoT to misbehave in the healthcare domain.
2) Study and evaluate AI models (1D CNN, LSTM, DT, RF, GB, and SVM) for detecting cybersecurity anomalies in the healthcare domain, using multi-class approach.
3) Analyzing the results of three IoT datasets (TON_IoT, Edge-IIoT and UNW-NB15) with the six AI models mentioned in (2) above, which is scarce in literature. To the best of our knowledge, only one research analyses them together, with deep learning techniques.
4) Integrating the IPFS-blockchain system to secure IoHT data, and checking for cybersecurity anomalies with

the selected AI models, thereby providing tamperproof data.

5) Providing more insight to researchers who are primarily interested in medical IoT.

In the rest of the paper, Section II summarizes the applications of AI models and BCT in analyzing their effectiveness for identifying and preventing cybersecurity threats in medical IoT systems. Section III explains the sample-gathering procedure and AI models applied in this study, as well as the integration of IPFS-BCT. Section IV and V describes the evaluation of the obtained results. The last section concludes our research.

II. LITERATURE REVIEW

A. AI ANOMALY DETECTION

According to Kumar et al. [13], a common technique for mitigating cybersecurity threats in medical IoT systems is the use of IDS (Intrusion Detection Systems). Naveed et al. [14] defined an IDS as a network-based system that constantly watches the transfer of packets to prevent unauthorized tasks from occurring. They are usually the secondary layer of performing network routines for the detection of anomalies [15]. IDS can monitor network traffic in real time and identify potential attacks, allowing for timely responses to prevent the attack from causing harm [16]. Research on intrusion detection is becoming more and more crucial, given the rise in IoT machines connected to a network. Thus, collecting and handling network intrusion datasets is essential for training and assessing various attack detection techniques [17].

Anomalous intrusion detection is currently anticipated by the academic/expert domain as a viable security solution that can significantly contribute to defending IoT networks [18]. Anomaly detection algorithms are models used to detect malicious activities in healthcare systems. Anomaly detection algorithms can detect abnormal network traffic or suspicious behavior patterns in the system, which can then be used to trigger alerts or take other preventive degrees [19]. According to Ashraf et al. [20], this technique is the most effective defense strategy for identifying and detecting new attacks in smart city networks. As an IDS, it generates a set of signature logs based on the available data and detects deviations from the identified signature as anomalies or unexpected events [21]. While traditional IDS lack the ability to detect unseen anomalies, AI-based IDS can detect unknown [22] or unseen anomalies. As technology evolves, it is necessary to incorporate AI into these systems.

Shahin et al. [23] proposed a framework to identify abnormal behaviors in the packet data of industrial IoT sensors. The models also include XGBoost and AdaBoost. Weinger et al. [24] focused on investigating the application of data augmentation to overcome challenges and enhance the detection efficiency in anomaly detection tasks using IoT datasets. Through extensive experiments conducted on three available IoT datasets, one of which is the TON-IoT dataset, significant performance improvements of up to 22.9% were observed when employing data augmentation compared to a baseline approach that did not utilize data augmentation.

Tareq et al. [25] analyzed two intelligent network models, namely DenseNet and Inception Time, for the detection of cyber-attacks using an integrated classification method. The performance of these models was assessed on three different datasets by conducting extensive simulations. With the TON-IoT dataset, the DenseNet model achieved a high accuracy of almost 100% for Windows 10, while the Inception Time model achieved a perfect accuracy of 100% for the same operating system. Latif et al. [26] adopted a dense random neural network (DnRaNN) for intrusion detection in IoT systems. The model was practically designed for resource-limited IoT networks as a result of its improved ability to generalize and its distributed nature. Extensive experiments were conducted using the TON_IoT dataset to evaluate the performance of the proposed model. Guo [27] proposed an IDS using the TON_IoT network dataset. In this work, ten AI models were evaluated, and the XGBoost model outperformed the other AI models. These results demonstrate the high performance of the proposed model and highlight the strengths of using the XGBoost model for detecting intrusions in IoT networks.

B. BCT ANOMALY DETECTION

Ordinary IoHTs are limited in resources and may lack intelligence. Hence, cyber attackers may take advantage of IoHT and their data points. To resolve this, Mishra [11] proposed a framework to detect and predict cyber-attacks in an accurate and efficient manner using a hybrid decision tree and five (5) other models on two datasets. The system, which combines BCT and machine learning for anomaly identification, was tested on a few datasets, obtaining close to 100% accuracy. Although this work is similar to our work, binary classification was used to analyze the AI models.

Kerrison et al. [28] proposed a system that combines IoHT with a secret BCT specifically for remote health tracking applications. The choice of a secret BCT approach was purposeful, with the goal of creating a controlled environment judged more suitable for healthcare settings than a public blockchain. Two different network frameworks were employed for device authorization and large-scale data transfers, and lightweight data transmission and event notifications comprised the operational structure. These frameworks used the same encrypted decision parameters. The work focuses more on communication problems than protecting IoHT data from cyber anomalies. Šarac et al. [3] presented a method for augmenting the security gateway architecture of IoT devices with BCT in order to achieve decentralization and authentication. The aim was to address the current shortcomings in anonymity and flexibility in IoT infrastructure. However, there was no practical implementation of AI, and the authors focused on using BCT to build an interface for IoT security. Rajasekaran et al. [29] introduced a privacy-preserving authentication scheme underpinned by blockchain to enable efficient patient authentication without reliance on a certified entity. The system was developed to prevent patient re-authentication in scenarios involving communication with multiple doctors. It focuses only on the patient aspect of the system, while everyone connected on the system should be authenticated. A two-level privacy strategy and an intrusion detection scheme serve as the foundation for the system proposed by Kumar et al. [30]. In a two-level privacy scheme, firstly, Principal Component Analysis (PCA) was utilized to convert raw IoT data into a new shape, and a blockchain module was built to securely transport the data. The authors presented a centralized, privacy-preserving, and secure framework that focused on smart cities. As a result of the voluminous data generated by IoT in smart cities, centralized storage is not suitable. Therefore, it is necessary to implement a decentralized storage framework.

These researchers focus on either of the technologies being studied (AI or BCT) in this work, except Mishra [11], to build an IDS for cybersecurity anomaly detection. We present the integration of both technologies using a decentralized approach. IPFS has been used with a specific smart contract algorithm to simplify the integration process. Most researchers generally rely on the simulation of single datasets to perform AI analysis. This does not totally ensure the validity of the AI models used. The selected models in this work were used to analyze three different datasets with different varieties of target data. It proves that these models can be effectively deployed for real-life applications. Also, the results presented in these studies provided binary classification except in a few cases. Furthermore, the existing literature does not provide enough guidance for integrating AI with BCT. As a result of the decentralized nature of blockchain, the most common challenges for the integration of these technologies are regulatory compliance and scalability. To resolve this, the tamperproof nature of BCT in this work enforces access control for managing IoHT data and, in turn, maintains regulatory compliance. The IPFS resolves the scalability problem by providing decentralized storage for IoHT data. In another light, deepfake anomaly detection will enhance authenticity in cybersecurity by managing large data and ensuring safe network environments. Kumar and Kundu [31] stated that deep learning algorithms have made it easier to manipulate digital content, giving rise to the phenomenon known as "DeepFake" (DF). Applying it to cybersecurity will help avoid social engineering attacks and ensure that digital content is genuine.

Evaluating detection in IoHT has true potential, and AI plays a crucial role in extracting valuable information from the vast amount of data collected. AI, on its own, has the ability, if properly modeled, to improve IoHT data security by denying cyber intruders access to the system preventing data modification and other forms of cyber-attacks [2]. One way to achieve this proper AI model for the above task is to critically analyze the complex datasets obtained from IoHT and other interconnected systems. While AI models are capable of analyzing vast amounts of data [32] and identifying patterns indicative of anomalies, they may still encounter limitations. One such limitation is the potential vulnerability of AI models to adversarial attacks or manipulation, where malicious actors deliberately craft input data to deceive the AI system and evade detection. By combining blockchain technology with strong cybersecurity and AI, IoHT can strengthen its security framework, take advantage of insightful data, reduce operating costs, and optimize workflows. This integrated approach not only strengthens digital ecosystem resilience but also improves organizational effectiveness in the face of changing technological landscapes.

III. METHODOLOGY

In this section, we analyze the methodology employed for our simulations. In this work, we have gone further to analyze the CNN and SVM AI models for our simulation, considering the detection of abnormal IoT behavior. Hence, these models were chosen based on our previous work [7], which serves as a background for this study. We also considered using three datasets, the TON_IoT, Edge-IIoT, and UNSW-NB15 datasets, on other AI models, including decision trees (DT), random forest (RF), gradient boosting (GB), and long short-term memory (LSTM). In the final stage of simulation, BCT was integrated to secure and validate the AI models. These datasets are detailed in Table 1, Table 2, and Table 3.

TABLE 1. TON_IoT dataset details.

Title	TON_IoT- Dataset
Reference	https://research.unsw.edu.au/projects/toniot-datasets
Abnormal behavior	DoS, DDoS, Mitm, XSS, Injection, Password, Scanning
Normal behavior	Normal
Target machine	Windows OS
Train_Test ratio	80:20

A. MATERIALS AND DATA

- TON_IoT: The TON_IoT data collection is a brand-new one created to analyze the effectiveness and precision of AI-based cybersecurity solutions for IoT/IIoT (Intelligent Internet of Things) networks. They comprise information gathered from a series of mainstream, such as network traffic, operating systems, and telemetry data from IoT and IIoT devices. The datasets were obtained from a sizable testbed network built at the UNSW Canberra Cyber IoT Lab. They are built on a testbed network

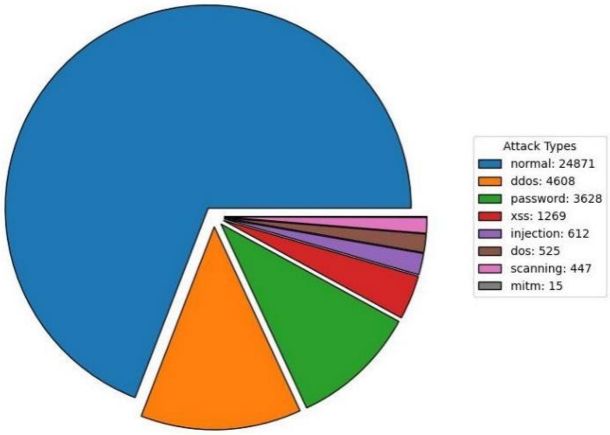


FIGURE 2. Sum total of behaviors in the TON_IoT dataset.

TABLE 2. Edge-IIoT dataset details.

Title	Edge_IIoT - Dataset
Reference	https://www.kaggle.com/datasets/sibasispradhan/edge-iiotset-dataset?select=DNN-EdgeIIoT-dataset.csv
Abnormal behavior	MITM, Uploading, Ransomware, SQL_injection, DDoS_HTTP, DDoS_TCP, Password, Port_Scanning, Vulnerability_scanner, Backdoor, XSS, Fingerprinting, DDoS_UDP, DDoS_ICMP
Normal behavior	Normal
Target machine	Windows OS
Train_Test ratio	80:20

that has SDN, NVF, and SO characteristics and were designed to be realistic. The datasets were obtained by parallel processing in order to gather labeled data on regular events and cyberattacks [33] for Windows operating systems [34]. Table 1 summarizes the TON_IoT data collection.

The TON_IoT dataset was fully described by Moustafa [33]. The selected Windows OS csv file comprises 127 features, with 35976 samples and 7 abnormal classes, which may be referred to as cyber-attacks and a normal class. The normal behavior is the exact same pattern or service the IoHT device or application is supposed to render. The abnormal behavior occurs when the IoHT device or application renders a service or presents a pattern that is different from the regular. Fig. 2 shows the sum total of each behavior available in the TON_IoT dataset.

- Edge_IIoT: This dataset was generated by Ferrag et al. [35], including fourteen (14) types of behaviors, which are grouped into 5 main types (DoS/DDoS, Information gathering, MITM, injection, and malware attacks).
The total number of samples available in this dataset is approximately 2,219,201. The sum total of each behavior is seen in Fig. 3, where some of the behavior names have been shortened.

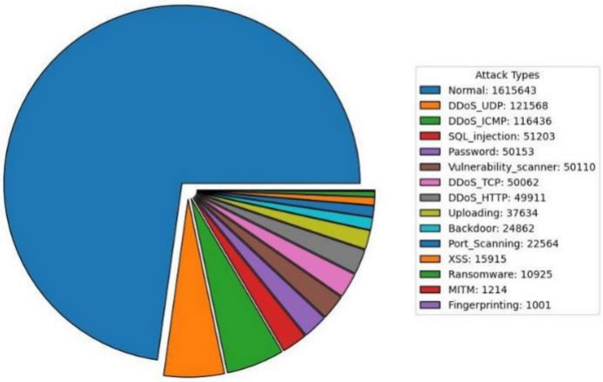


FIGURE 3. Sum total of behaviors in the Edge_IIoT dataset.

- UNSW-NB15: This dataset consists of ten (10) behaviors, having 9 anomalies and 1 normal behavior [36].

TABLE 3. UNSW-NB15 dataset details.

Title	UNSW-NB15 - Dataset
Reference	https://research.unsw.edu.au/projects/unsw-nb15-dataset
Abnormal behavior	Backdoor, Analysis, Fuzzers, Shellcode, Reconnaissance, Exploits, DoS, Worms, Generic
Normal behavior	Normal
Target machine	Windows OS
Train_Test ratio	80:20

It has very large inputs, approximately 2,540,044 when combined together. The author of the dataset has partitioned train and test samples, which are 175,341 and 82,332, respectively [37]. The distribution of behaviors is seen in Fig. 4, based on the Train_Test dataset.

B. DESCRIPTION OF IDENTIFIED BEHAVIORS

The following behaviors have been identified in all three datasets:

1) Normal: This refers to the expected behavior of systems and networks, which is completely different from malicious attacks (abnormal behavior).
2) DDoS: The DDoS attack occurs when there is a denial of service on the network. It results in the denial of access for a particular device or the IoHT application itself [7]. Considering our use case, DDoS attacks can

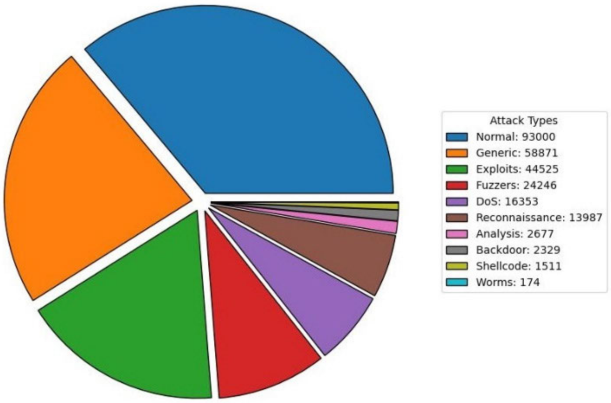


FIGURE 4. Sum total of behaviors in the UNSW-NB15 dataset.

make IoHT resources to be unavailable [38]. The forms of DDoS attacks include DDoS_HTTP, DDoS_TCP, DDoS_UDP, and DDoS_ICMP [35].

3) DoS: Denial of service attacks are similar to DDoS. They are the most common types of IoT anomalies [3].
4) MITM Attacks: Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when an attacker infiltrates a bilateral transaction and steals information from both parties [39].
5) Injection: The entire security of the IoHT network may be threatened by cyber attackers attempting to introduce malicious segments, commands, or answers within its domain [38]. Another form of this attack includes exploits and shellcode.
6) Password Attack: This attack may be in the form of brute force, phishing, or dictionary attacks. These majorly target individual or system verification in terms of authentication [40] on IoHT applications. Another form of this attack is a backdoor attack [35].
7) Scanning Attack: cyber attackers routinely evaluate IoHT to collect network-related data in preparation for launching advanced attacks aimed at compromising the IoHT's security. IP address scanning, port scanning, and version scanning are all common scanning strategies used to gather information about computer networks [38].
8) Cross-Site Scripting: Cross-Site Scripting (XSS) is a cyber-attack in programming arising from improper sanitization of user input data. This flaw allows attackers to exploit the vulnerability by injecting unfiltered scripting code into a web application [41]. The most common website threat is cross-site scripting (XSS) attacks. Other forms of this attack include SQL injection [42] and uploading attack [35].
9) Information collection: This form of attack includes collecting intelligent information about the target component. They include port scanning, vulnerability scanners, fingerprinting [35] analysis, reconnaissance, worms, and fuzzers.

C. DATA PRE-PROCESSING

In the pre-processing phase, we first performed basic data cleaning by removing values that were unavailable, applying label encoders to the target column, reducing the features, and finally performing feature scaling.

1) Removing null values: A few values were missing from the TON_IoT dataset; hence, these were removed to avoid conflicts while analyzing the dataset.
2) Label encoders: This step was mainly performed on the multi-class label feature. The TON_IoT dataset includes a label that classifies normal behavior as 0 and all abnormal behaviors as 1. This couldn't be considered the final target; hence, we considered the multi-class label feature, which was in textual format. Label encoding was done to convert the textual classes to numeric values from 0 to 8, which is more suitable for AI models.
3) Feature Reduction: The features were reduced from 127 to 47 by removing features whose values could not be converted to float datatype. The essence of reducing the features in this manner was to ensure machine learning compatibility since statistical data is most appropriate for the selected AI models.
4) Feature scaling: This was done was done using normalization (see Fig. 5). It involves transforming features to a standard scale and is considered a pre-processing [43] technique in the AI domain. The primary objective of normalization is to adjust the values of numbered features in the input vector to a specific range of values [44]. The aim is to enhance the accuracy of datasets, which is achieved through various types of normalization techniques. The MinMax normalization technique [43] was used in our work, which can be calculated based on Equation (1). Where $s_i' =$ the normalized output, $s_i =$ the value to be normalized, $X_{min} =$ the minimum value, $X_{max} =$ the maximum value. The formula first finds the range between s_i and X_{min}, after which the result is divided by the difference between X_{max} and X_{min}. The final result must fall between 0 and 1.

$$s_i' = \frac{(s_i - Xmin)}{(Xmax - Xmin)} \tag{1}$$

D. EXPERIMENTAL DESIGN FOR SELECTED AI MODELS

The experimental design analyses the three datasets of TON_IOT, Edge-IIoT, and UNSW-NB15 datasets using six (6) AI models – 1D Convolutional Neural Networks, Support Vector Machines, Decision Tree, Gradient Boosting, Random Forest, and Long-Short Term Memory Neural Networks, as seen in Fig. 5. The output is the target data in 8 classes for TON_IoT, 15 classes for Edge_IIoT, and 10 classes for UNSW-NB15, where there is one normal behavior and an abnormal behavior that may be in the defined classes. The following section explains the utilized 6 AI models in our work.

The datasets were divided into two sections, 80% of the dataset was used for training, and 20% was used for testing. This was done using random selection in order to avoid bias. This approach is crucial for preventing overfitting, a condition where a model performs exceptionally well on the training data but fails to generalize to new, unseen data. By introducing randomness in the selection of training and testing instances it ensures that the model learns from diverse examples, improving its ability to make accurate predictions on new data. Given that X is the dataset, let X_{train} be the data to be trained, and X_{test} be the data to be tested; in terms of programming function, random selection can be expressed as seen in Equation 2:

$$X_{train}X_{test} = \text{train\_test\_split}(X, \text{test}_{size} = r, \text{randomselection} = s) \quad (2)$$

where r = the percentage assigned to X_{test}, and s = random value to be generated.

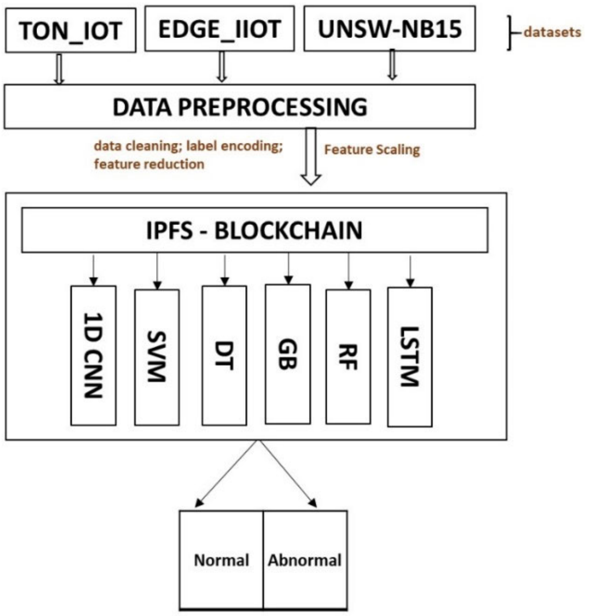


FIGURE 5. Workflow of evaluated AI models and BCT.

The train_test ratio was split into 80:20 to provide the AI models with a good balance of learning and validating samples, which are selected randomly and balanced with the resampling technique.

All experiments were performed on a Windows 11 PC, with Intel(R) Core(TM) i7- 1250U CPU at 1.10 GHz and 16 GB RAM. The implementation of machine learning models and blockchain is performed using Python and Solidity.

E. MACHINE LEARNING TOOLS

1) 1-Dimensional Convolutional Neural Networks: A 1D CNN is frequently used for processing and studying one-dimensional data, such as time-series signals. According to Kiranyaz et al. [45], it recently came to light, and it is excellent for anomaly detection. It uses pooling layers [32] to make the feature maps less dimensional and convolutional layers to extract features from the input data. Contrasting this with 2D CNN, 1D CNN excels in capturing patterns in sequential information, while 2D CNN demonstrates proficiency in discerning spatial relationships within multidimensional datasets. 2D CNN is adept at processing two-dimensional structured data, such as images [46], employing convolutional operations across both width and height dimensions. The 1D CNN used comprises the input, conv1D (4), dropout, MaxPooling1D, and dense layers.
2) Support Vector Machines (SVM): is a supervised ML model that utilizes a separating hyperplane. SVMs aim to find the hyperplane that best maximizes [47] the margin of a dataset. The algorithm draws a line or a hyperplane to divide data into classifications [48]. To reformulate data, it leverages a mathematical function known as the kernel. Following this change, the SVM algorithm determines the best boundary between the labels. It primarily performs a series of transformations in order to discover a solution to segregate the data based on the labels or outputs specified [49].
3) Decision Trees (DT): are created using an algorithmic model that defines the most effective way to divide a dataset based on specific characteristics [22]. The purpose is to generate simple decision rules from the data features and graphically represent them in a decision tree [50]. The divide and conquer approach [9] are used to build the decision tree, which is simple to implement, but it may have issues with repeating and reproducing results.
4) Gradient Boosting (GB): GB is an ensemble [51] method primarily focused on the gradient boosting approach [47]. The GBM uses multiple learning algorithms as fundamental learners. This model utilizes boosting to create an ensemble of weak decision-tree learners periodically.
5) Random Forest (RF): RF is a model that may be used for either classification or regression. This essentially constitutes an assembly of decision trees [52]. In classification tasks, the Random Forest (RF) algorithm utilizes a majority voting approach, while for regression, it employs averaging. By aggregating predictions from multiple decision trees in this fashion, the RF algorithm reduces model variance and enhances overall performance. The two key hyperparameters of RF are the sum total of trees and randomly selected features or variables utilized to train each decision tree within the forest [53]. As the forest grows larger, the random forest classifier can handle missing data and avoid overfitting the model. It can also be employed to create classifiers for categorical variables [47].

6) Long Short-Term Memory (LSTM): It refers to a particular kind of recurrent neural network that is an extremely efficient method for doing classification and regression tasks. Cell, input gate, output gate, and forget gate are the four main parts that build the architecture [54] of its model. Gradients are employed to update weights, but because the network is built to remember earlier errors, fewer iterations are required to achieve greater error minimization [9].

Each AI tool is trained with the hyperparameters (see Table 4), and the model is saved. The saved model is used for validation from the IPFS. The integration of the IPFS-BCT is briefly discussed in section IV.

F. ML HYPERPARAMETERS

This section states the hyperparameters for each AI model used in this study, as seen in Table 4.

TABLE 4. List of AI hyperparameters.

AI model	Hyperparameter
CNN	dropout rate=0.5, number of filters (16-64), and kernel size=2, optimizer=RMSprop, ReLU (rectified linear unit) activation function, epoch=3
SVM	linear kernel, and regularization = 1
DT	Default - criterion, splitter, max depth, min samples split and leaf, max features
GB	number of iterations with no change =5, validation fraction=0.2, and random state=100, learning rate=0.1
RF	number of estimators=10, max depth=10 and random state=100
LSTM	batch size=1, epoch=3, optimizer=Adam, loss function, input shape

The grid search was employed to systematically search through a pre-set set of hyperparameter values, evaluate the model's performance for each combination, and select the set of hyperparameters that produce the best results.

G. EVALUATION METRICS

The common standards employed to analyze various AI models include accuracy, precision, recall, and F1-score. Although accuracy is frequently used, it cannot always be relied upon, as it simply denotes the percentage of correct predictions. Precision measures the degree of correct valid (positive) predictions, while recall indicates how accurately the model identifies true variables. Precautions were taken to ensure that the datasets were balanced, hence the use of the following metrics:

1) Precision: This metric straightforwardly indicates the "relevance count of selected data items." In essence, it quantifies the accuracy of the algorithm's positive predictions by determining the actual positivity within the selected observations, as seen in Equation 3:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

2) Recall: The metric under consideration delineates the "quantification of pertinent data elements chosen." Specifically, it addresses the subset of positive instances within the observed dataset and examines the algorithm's capacity to accurately predict this subset, as seen in Equation 4:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

3) F1-Score: It incorporates both precision and recall to assess the performance of an algorithm (see Equation 5).

$$\text{F1} = \frac{2.\text{PR}}{\text{P} + \text{R}} \tag{5}$$

4) Accuracy: Evaluation of algorithm performance in classification problems often leans heavily on accuracy, frequently regarded as the primary and, perhaps, the foremost criterion. This metric is articulated as the proportion of correctly classified data instances to the overall number of observations (see Equation 6).

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{6}$$

where TP = True classification of the actual value, and it is True
TN = True classification of the actual value, but it is False
FN = False classification, but the actual value is True.
FP = True classification of the actual value but is False

IV. BLOCKCHAIN INTEGRATION

This section highlights blockchain integration with AI, which uses a smart contract algorithm to secure data.

In this work, the smart contracts by BCT were used to secure and validate the AI models before the actual detection of IoT behavior was done. Smart contracts function as a platform for automating operations, enforcing business logic, and facilitating safe interactions between IoHT sensors and the blockchain network. The smart contracts are independent agreements contained inside the blockchain structure. Because they are intrinsically resistant to tampering and irreversible, smart contracts provide a means for automating and enforcing agreements among participating parties [55]. The smart contract algorithm is summarized in two (2) major steps, as seen in the algorithm (see Table 5). The algorithm provides a security and tamperproof system for managing the IoHT data.

The selected AI models are simulated and with data stored on the IPFS, which are deployed on the blockchain (see Fig. 5), after the actual execution of security implementation is carried out. The algorithm employs cryptography [10] by hashing data entries to the blockchain. This hashed data is

TABLE 5. Smart contract algorithm.

1	Save encrypted CID and hash
2	Retrieve the encrypted CID

now processed before the blockchain calls each AI model for validation. The hashing scheme is built around SHA-3, a new way to keep data safe. In 2012, a group picked Keccak as the best way to be used in SHA-3. This makes Keccak the top choice for making safe hash values [56]. On the other hand, the Python fernet library was used to encrypt the required data following the Advanced Encryption Standards (AES) format. This is a symmetric encryption scheme that makes use of one key to encrypt and decrypt data. While the main focus of this work is the use of AI models to detect cyber anomalies in IoHT data, the blockchain logic in this work is used to secure the dataset, in which IPFS has also been adopted, as seen in Fig. 6.

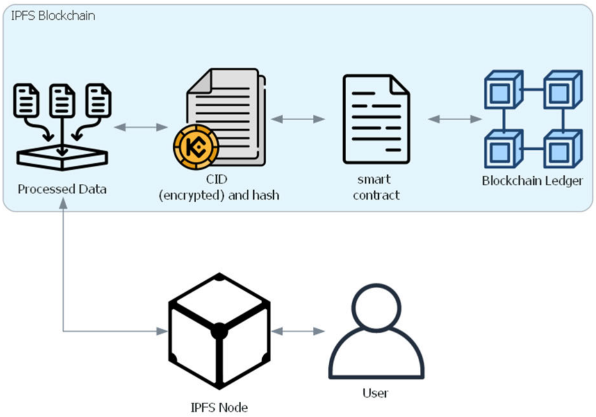


FIGURE 6. Blockchain integration.

After the data pre-processing phase, the processed data is stored on the IPFS. The generated CID is then encrypted, hashed, and saved on the blockchain via the smart contract. Hence, once the user is connected, the hashed CID is decrypted, and the original CID can now be referenced to perform the AI validation, and the tamperproof result can be obtained. The tamperproof works by comparing the initial behavior (normal or abnormal with the defined anomalies) to the predicted behavior in order to state the tampered results.

The whole process ensures that the smart contract is used to secure the IoHT data. This process provides the tamperproof data used to validate the AI models before the actual detection of behavior is done.

V. SIMULATION RESULTS AND COMPARISON

A. RESULTS

1) TON_IoT Dataset: For each model, the precision, recall, and F1-score have been presented for each target class, as well as the accuracy for each model, as seen in Tables 6, 7, and 8. The CNN model's accuracy, precision, recall, and F1-score are 85%, 93%,85%, and 88% respectively. This model could not classify injection, MITM, and scanning attacks. The CNN model can only classify some instances of DoS, password, and DDoS attacks. The SVM obtained maximum results of 100% each for accuracy, precision, recall, and F1-score, respectively. This shows that the SVM model can accurately classify all instances for each class. With the DT model, only a few instances of the scanning attack are not appropriately classified. The model accurately classifies the instances of other classes. The accuracy, precision, recall, and F1 score are 100% each. The GB model can classify about 0.5 instances of the MITM attack. Only a few instances of the scanning attack could not be identified. All other classes are identified accurately. The accuracy, precision, recall, and F1 score are 100% each. Aside from the scanning attack, the RF model accurately identifies the other target classes. It is only a few instances of the scanning attacks that were not identified. The accuracy, precision, recall, and f1-score are 100% each. Considering the LSTM, the classification results show that the model performed well in detecting the NORMAL and XSS classes but struggled with accurately classifying the DOS, MITM, and SCANNING classes. The model achieved moderate accuracy, precision, recall, and F1-score of 87%, 89%, 87%, and 87%, respectively, across all classes.
2) Edge_IIoT Dataset: The results, as seen in Tables 6 and 7 show that the 1D CNN and LSTM (85% and 74%, respectively) perform poorly while the traditional ML algorithm obtained optimal results, as that of the TON_IoT dataset. The results were obtained using 1,775,360 samples for training and 443,840 samples for testing, along with 39 features.
3) UNSW-NB15 Dataset: The results produced by this dataset are minimal when compared to the TON_IoT and Edge_IIoT datasets. Since there was a partition of train and test samples, 206,138 samples were used for training, and 5,134 samples were used for testing, Along with 44 features. While the CNN and LSTM models perform better than the Edge_IIoT dataset, the traditional AI models (SVM, DT, GB, and RF) obtained 89%, 87%, 88%, and 87% accuracy, respectively.

Table 6 describes the overall results across the selected AI models for each of the datasets. The SMOTE resampling technique was used to balance the dataset, where necessary, in the training phase. This provides a straightforward accurate result and makes it valid. On the other hand, more comprehensive details about the precision, recall, and F1-score for each type of cybersecurity behavior are seen in Table 7.

The traditional machine learning algorithms depict a consistent flow of results with the datasets. The other two datasets (Edge_IIoT and UNSW-NB15) presented in this study obtained less results for the chosen AI model, as seen in

TABLE 6. Accuracy report for evaluated AI models.

Dataset	1D CNN	SVM	DT	GB	RF	LSTM
TON_IOT	85	100	100	100	100	87
Edge_IIoT	85	98	97	96	83	74
UNSW-NB15	63	89	87	88	87	74

Fig. 7, the performance report analysis. Table 7, on the other hand, gives the breakdown for each behavior's precision, recall, and F1 score per dataset.

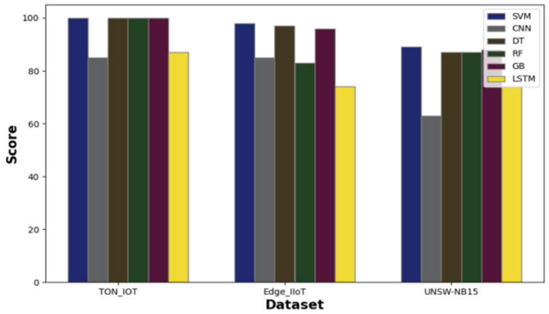


FIGURE 7. Datasets Performance evaluation.

The research work of Tareq et al. [25] is the only work so far that analyzed the three datasets. Deep learning was used and the results were 99.9%, 94.94% and 98.4% accuracy, respectively, for TON_IoT, Edge-IIoT, and UNSW-NB15 datasets. Other works reference the datasets differently. Akuthota and Bhargava [36], although they used binary classification, obtained 89.97% and 98.68% using SVM and RF, respectively, for UNSW-NB15. Considering the Edge_IIoT dataset, Laiq et al. [57] specifically focused on the different forms of DDoS and used XGBoost to obtain an accuracy of 99.88%. With Multiclassification, the SVM model obtained 100%, 98%, and 89% accuracy, respectively, for Ton_IoT, Edge-IIoT and UNSW-NB15 respectively.

The integration of the BCT technology is an added advantage as it provides a means to validate the selected AI models and secure data being received on the IoHT.

B. COMPARISON OF RESULTS TO LITERATURE REVIEW ON TON_IoT

In comparison to Table 8, Shahin et al. [23] considered Attention-based LSTM, CNN, Adaboost, and XGBoost and achieved an accuracy of 95.97%. It had a precision and recall of 95.68% and 95.74%, respectively. Weinger et al. [24] used Federated Learning (FL) in their study and achieved an accuracy of 89.32%. Its precision, recall, and F1-score were 80.54%, 71.38%, and 73.25% respectively. The model used 17 features for classification. Tareq et al. [25] adopted DenseNet and Inception Time in their study and achieved an accuracy of 99.9%. Both precision and recall were 99.9%, and the F1-score was 98.57%. Latif et al. [26] used a lightweight, dense random neural network (DnRaNN) and achieved an accuracy of 99.15%. It had a precision, recall, and F1-score of 99.23%, 99.07%, and 99.27%, respectively. Guo [27] applied XGBoost and achieved a high accuracy of 99.93%; this value was the same for the precision, recall, and F1 score after considering 45 features.

The work of Kumar et al. [30] is almost similar to our work in the full scope. Gradient Boosting was the main AI algorithm used in their work, with an accuracy of 98.38%. The SVM model outperformed the other models used in this study, achieving flawless accuracy, precision, recall, and F1-score. It also utilized a larger set of features compared to the other models. Aside from our work and Kumar et al. [30], none of these studies integrated blockchain technology for security purposes. Ours improves on their research, as we have integrated the BCT and taken a different approach in comparison to Kumar et al. [30].

Ferag et al. [35] carried out the experiments with Multiple datasets, including Edge_IIoT. An analysis was performed on the Edge_IIoT dataset with 3 stages of classes (2, 6, and 15) using traditional ML algorithms and federated learning. With 15 classes, the SVM obtained 77.61%, DT obtained 67.11%, and RF obtained 80.83%. Saeed et al. [58] used an ensemble learning hybrid approach on multiple datasets, including the UNSW_NB2015 dataset, which obtained an accuracy of 99.9%. Roy and Singh [59] extracted 20 features with the UNSW-NB15 dataset and applied the Reduced Error Pruning Tree (REPTree) to obtain 99.94% accuracy. Nuaimi et al. [42] performed both binary and multi-classification on the Edge_IIoT dataset with 6 models different from those used in this study. The AI models include two decision tree learners, BayesNet, AdBoost, and LogitBoost, and an Attribute-selected classifier (ASC). The highest accuracy obtained for the binary and multi-classification is 99.55% and 92.92%, respectively, with the decision tree classifiers.

The research work of Tareq et al. [25] is the only work so far that analyzed the three datasets. Deep learning was used, and the results were 99.9%, 94.94%, and 98.4% accuracy, respectively, for the TON_IoT, Edge_IIoT, and UNSWNB15 datasets. Other works reference the datasets differently. Akuthota and Bhargava [36], although they used binary classification, obtained 89.97% and 98.68% using SVM and RF, respectively, for UNSW-NB15. Considering the Edge_IIoT dataset, Laiq et al. [57] specifically focused on the different forms of DDoS and used XGBoost to obtain an accuracy of 99.88%. With Multiclassification, the SVM model obtained 100%, 98%, and 89% accuracy for TON_IoT, Edge_IIoT, and UNSW-NB15, respectively.

Although these works are related to cybersecurity, none of them focused on applying it in the healthcare domain. Further discussion on how BCT was integrated into our work is given in section VI.

VI. DISCUSSIONS

The current research field is exploring BCT technologies in different IoT domains. The current literature is exploring BCT in healthcare domains such as rural patient health

TABLE 7. Classification report for selected AI models.

TON_IoT Dataset																		
Class	1D CNN (100%)			SVM (100%)			DT (100%)			GB (100%)			RF (100%)			LSTM (100%)		
	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score
DDOS	100	73	84	100	100	100	100	100	100	100	100	100	100	100	100	93	69	80
DOS	7	19	11	100	100	100	100	100	100	100	99	100	100	100	100	15	31	20
INJECTION	0	0	0	100	100	100	100	100	100	100	100	100	100	100	100	0	0	0
MITM	0	0	0	100	100	100	100	100	100	50	67	57	100	100	100	2	50	5
NORMAL	99	92	95	100	100	100	100	100	100	100	100	100	100	100	100	93	99	96
PASSWORD	79	96	86	100	100	100	100	100	100	100	100	100	100	100	100	83	54	65
SCANNING	0	0	0	100	100	100	98	100	99	97	100	99	97	100	99	0	0	0
XSS	99	54	70	100	100	100	100	100	100	100	100	100	100	100	100	100	94	97
Edge_IIoT Dataset																		
NORMAL	0	0	0	98	94	96	100	100	100	98	98	98	98	97	97	0	0	0
MITM	0	0	0	100	100	100	100	100	100	100	100	100	100	100	100	0	0	0
UPLOADING	97	98	98	99	100	99	100	100	100	100	100	100	100	100	100	87	38	53
RANSOMWARE	75	66	70	99	100	99	100	100	100	100	100	100	99	100	100	0	0	0
SQL_INJECTION	86	99	92	100	100	100	100	100	100	100	100	100	100	100	100	61	43	51
DDOS_HTTP	1	7	2	100	33	50	100	100	100	33	33	33	100	100	100	0	13	0
DDOS_TCP	1	50	3	100	100	100	100	100	100	100	100	100	100	100	100	0	0	0
PASSWORD	95	97	96	100	100	100	100	100	100	100	100	100	100	100	100	97	99	98
PORT_SCANNING	9	14	11	100	100	100	100	100	100	100	100	100	100	100	100	25	18	21

monitoring [28], efficient patient authentication [29], IoT gateway authentication, and decentralization [3]. Implementing BCT in our work with the use of smart contracts into IoHT has the potential to improve both efficiency and security.

Tables 6 and 7 highlight the persistent outperformance of SVM, DT, GB, and RF models over 1D CNN and LSTM models, considering all three datasets. The SVM is preferred because it was selected with CNN from our previous work [7].

TABLE 7. *(Continued.)* Classification report for selected AI models.

VULNERABILITY_ SCANNER	43	41	42	94	90	92	100	100	100	99	97	98	100	100	100	4	5	4
BACKDOOR	1	6	2	81	88	85	100	100	100	94	100	97	91	91	91	4	23	8
XSS	17	14	16	100	100	100	100	100	100	100	100	100	100	100	100	0	0	0
FINGERPRINTING	7	2	3	100	100	100	100	100	100	100	100	100	100	100	100	0	0	0
DDOS_UDP	91	29	44	97	99	98	100	100	100	100	100	100	99	100	100	0	0	0
DDOS_ICMP	0	0	0	98	92	95	100	100	100	100	100	100	100	98	99	0	0	0
UNSW-NB15 Dataset																		
NORMAL	0	0	0	88	8	15	22	21	21	68	15	24	92	13	23	100	1	2
BACKDOOR	0	0	0	0	0	0	13	12	13	41	11	17	100	1	3	0	0	0
ANALYSIS	36	15	22	37	1	1	31	31	31	42	26	32	41	6	11	0	0	0
FUZZERS	59	67	63	58	89	70	71	70	70	65	86	74	60	93	73	56	75	64
SHELLCODE	46	68	55	76	74	75	83	84	83	90	84	87	85	85	85	33	62	43
RECONNAISSANC E	78	89	83	99	98	99	98	98	98	100	98	99	100	98	99	81	82	81
EXPLOITS	92	96	94	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
DOS	0	0	0	65	66	66	76	80	78	92	77	84	93	72	81	0	0	0
WORMS	0	0	0	75	4	7	60	59	59	66	71	68	68	20	31	0	0	0
GENERIC	0	0	0	50	14	22	29	57	38	44	57	50	100	14	25	0	0	0

The 1D-CNN could outperform the conventional machine learning models with higher efficacy in time-series data, where the neighboring kernels capture the relevant features among the consecutive samples. Even though the considered datasets comprise time stamps, each stamp has several attributes that make them non-time series for each instance. Despite the efficacy of the 1D-CNN in classifying complex patterns or data, its performance could decrease when data is sparse due to extracting the neighboring non-relevant features [60]. This limitation of the 1D-CNN also occurs in other deep learning models, such as LSTM. The LSTM aims to extract the consecutive features of time-series data and to remember the relevant features within long and short periods. The sparse or non-time series data could cause a deficiency in establishing strong relations within the extracted features to obtain higher classification rates.

On the other hand, the SVM is an effective machine-learning model that uses the closest class samples to determine support vectors on the projected hyperplane and to draw a decision line for binary or multiclass problems. The projected data provides reasonable classification rates, making it an effective model for different data types. SVMs also fit data without overfitting, which improves the generalization compared to the deep learning models. Notably, incorporating blockchain into the SVM model is remarkably effective, yielding ideal scores almost throughout the analyzed parameters. These

TABLE 8. Comparison of results based on literature review, TON_IoT.

Reference	Accuracy (100%)	Precision (100%)	Recall (100%)	F1-score (100%)	No. of Feat.
Shahin et al. [23]	-	95.97%	95.68%	95.74%	-
Weinger et al. [24]	89.32	80.54	71.38	73.25	17
Tareq et al. [25]	99.9	99.9	98.57	98.57	-
Latif et al. [26]	99.15	99.23	99.07	99.27	-
Guo [27]	99.93	99.93	99.93	99.93	45
Kumar et al. [30]	98.38	95.32	-	94.80	19
Our Work (SVM + BCT)	100	100	100	100	47

TABLE 9. Comparison of results with SVM and other works.

Reference	Dataset	AI tool	Accuracy
Ferag et al. [35]	Edge_IIoT	SVM, DT, RF	77.61, 67.11, and 80.83
Saeed et al. [58]	UNSW-NB2015	Ensemble Learning	99.9
Tareq et al. [25]	TON_IoT, Edge_IIoT and UNSW-NB15	Deep learning	99.9, 94.94, and 98.4
Akuthota and Bhargava [36]	UNSW-NB15	SVM and RF	89.97 and 98.4
Roy and Singh [59]	UNSW-NB15	RepTree	99.94
Nuaimi et al. [42]	Edge_IIoT	PART and J48	99.55 and 92.92
Our Work (SVM + BCT)	100	100	100

findings support the current study's favorable placement in comparison to previous research, revealing the advances made in the field of intrusion detection through the combination of AI models with BCT.

The entire process was relatively slow due to the system's specifications and the local environment setup for this simulation. The actual data is encrypted on the blockchain. In the field of cybersecurity, encryption plays an important role by transforming information into an illegible format, accessible only to persons with the appropriate private key. This is especially critical within the AI-Blockchain ecosystem, given the vulnerability of data and the substantial worth associated with transactions. The integration of AI necessitates a more sophisticated approach to encryption to protect both input data and output results. To address this need, employing layered encryption methodologies becomes imperative. Advanced encryption techniques offer a promising solution by enabling computations on ciphertext without the need for decryption beforehand. This feature presents an appealing avenue for maintaining data privacy and authentication in AI operations conducted on an IPFS Ethereum Blockchain system, bringing about the following validations, in line with the works of other researchers from section II:

1) Data Privacy and Security: BCT ensures data security by incorporating cryptographic technologies. These methods of encryption use mathematical procedures to convert normal messages into unreadable formats, making it incomprehensible to those without authorization. Cryptographic security is a powerful barrier to prospective data breaches by hackers. Centralized systems, on the other hand, frequently store data in plain text, creating a vulnerability that makes it more vulnerable to unauthorized access and data theft [55]. Utilizing the IPFS implies that sensitive data is stored off-chain while the hash is stored on the blockchain, thereby enabling data to be updated, securing the data, and bringing about privacy.
2) Perform Decentralization: The decentralized nature of BCT indicates the absence of control by a single body. This decentralization feature improves security by enabling it to be more challenging for hostile actors to target and breach the system. Decentralized systems, including IPFS, disseminate data among several nodes, as opposed to centralized systems, which keep data on a single server, providing a vulnerability as a single point of failure. This distribution considerably complicates unauthorized access attempts by hackers to infiltrate the entire data set [55].
3) Validate the simulated AI models: Validation is intended to create trust in the cybersecurity architecture, resulting in a safe, dependable, and resilient environment for IoHT. It also assures stakeholders, including medical professionals, patients, and regulatory authorities, of the reliability of the established security measures. Validating the AI models in this manner confirms that they truly demonstrate resilience against various cyber threats and adapt to evolving security challenges, which is the most important aim of this work.

AI and BCT are two forms of technology that the current industry cannot do without, alongside the advancements of systems [61] in various sectors, not excluding healthcare. The build of these technologies will assist in mitigating cybersecurity issues in the long run. Aside from protecting IoHT data, these methods also ensure the security and reliability of data [4]. The blockchain's decentralized nature provides a secure database for sensitive and personal data. With digital signatures and the use of private keys, AI algorithms can operate on secure and valid data, resulting in less accurate outputs. The decentralized ledger of blockchain meticulously records transactions, instilling certainty and confidence in the decisions made. The process of logging relevant details on the blockchain ensures confidentiality, trust, and transparency. This also aids in the efficient decision-making output of the system without involving a third party or centralized authority. Combining many cybersecurity methods into one cohesive system offers all-around protection on critical networks and efficiently handles timing issues [62]. Through the integration of two powerful paradigms, this integration effectively guards against potential tampering with data and unauthorized access in highly sensitive domains. Fundamentally, the blockchain's unchangeable record improves sophisticated AI models, which are widely recognized for their remarkable accuracy in categorization jobs. Through this agreement, a secure framework that ensures the correctness and dependability of data transactions is created, supporting AI-driven predictions and classifications with a tamperproof audit trail. This feature also provides an additional layer of security for AI applications and helps to lessen the risks brought about by weakened central points and intentional manipulation.

Also this combination might seem complex, it also has the ability to monitor and detect cyber anomalies in the system. They can also be combined with IDS, a major cybersecurity framework for intrusion detection and tamper-proofing. IDS alerts network administrators once a breach is noted in the system. BCT can also support IDS by implementing a tamperproof log of transactions occurring in the network, again building transparency. This technique can be employed in other domains as well. The blockchain tamperproof technique (which was used in the simulation of this study) combined with AI initiates a landmark cybersecurity innovation, leading a new phase where data integrity and trust are the topmost priority. As organizations navigate an increasingly complex threat landscape, this symbiotic relationship between two pioneering technologies offers a beacon of hope, empowering stakeholders to safeguard their digital assets with unwavering confidence and resilience. Also, the nature of the features in a dataset greatly impacts the effectiveness of these models. AI models also need to be checked regularly to be in line with evolving cybersecurity issues. Carrying out this task may be cumbersome, even with aids from the required expertise. Therefore, finding sustainable and affordable methods to maintain and support current AI algorithms is an important area of research in medical IoT cybersecurity.

A. LIMITATIONS OF THE STUDY

Firstly, the materials found in the databases focused more on cybersecurity issues in agriculture, smart cities, maritime transport systems, industry, and general IoT issues. Only very few researches focused on healthcare IoT systems. Secondly, well-defined datasets are scarce and need proper data cleaning and pre-processing phases to be done before the primary simulation analysis can be performed. Thirdly, the system specification used to carry out the simulation made the simulation process very slow, as a regular Windows OS machine was used. The challenge of integrating blockchain via the available test networks is cumbersome [61]. A significant amount of time passed, primarily as ascribed to the process of code execution for this particular simulation. This is because there is not enough information [62] available on implementing the code aspect of the simulation.

VII. CONCLUSION

This study evaluates existing AI models for detecting anomalies in medical IoT, using TON_IoT not previously applied in the medical domain, as well as Edge_IIoT and UNSW-NB15. The focus was on validating the effectiveness of well-known AI models in the context of medical IoT cybersecurity while securing data with IPFS-BCT. The increasing prevalence of IoHT systems underscores the importance of ongoing research to enhance their ability to identify and mitigate cybersecurity risks. The integration of advanced machine learning models with BCT offers a promising approach to addressing security concerns while maintaining efficiency and adaptability. Despite challenges, research indicates that these technologies can effectively detect and manage cyberattacks. Among the evaluated models, the Support Vector Machine (SVM) performed optimally, achieving 100% accuracy with TON_IoT, 98% with Edge_IIoT, and 89% with UNSW-NB15 datasets. The integration of IPFS in BCT, particularly with the SVM model, yielded ideal results across all parameters, enhancing accuracy, reliability, and security in intrusion detection within IoHT environments. This study contributes valuable insights for future research, particularly in improving cybersecurity in healthcare. It is recommended to include prioritizing the integration of advanced machine learning models with BCT leveraging SVM with statistical IoHT data for enhanced anomaly detection, fostering collaboration among academia, healthcare, and regulatory authorities, and ensuring continuous monitoring and updating of AI models to address evolving cybersecurity threats.

INFORMED CONSENT STATEMENT

This study does not involve human participants, and all data used are obtained from secondary sources, ensuring no personal information or interaction is required.

DATA AVAILABILITY STATEMENT

The datasets utilized in this study, including TON-IoT, UNSW-NB15, and Edge_IIoT, are publicly available and openly accessible for research purposes. However, it is important to note that the code employed in our research is proprietary and cannot be shared due to confidentiality and intellectual property considerations. This code encompasses sensitive algorithms and proprietary methodologies that are fundamental to our research and cannot be disclosed at this time.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENT

OLUWASEUN PRISCILLA OLAWALE would like to thank her supervisor, Associate Professor. Dr. Sahar Ebadinezhad for providing insight and expertise that greatly assisted this research.

REFERENCES

[1] A. K. Tyagi, T. T. George, and G. Soni, "Blockchain-based cybersecurity in Internet of Medical Things (IoMT)-based assistive systems," in *AI-Based Digital Health Communication for Securing Assistive Systems*. Hershey, PA, USA: IGI Global, 2023, pp. 22–53, doi: 10.4018/978-1-6684-8938-3.ch002.

[2] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, Apr. 2019.

[3] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Rep.*, vol. 7, pp. 8075–8082, Nov. 2021.

[4] D. Elangovan, C. S. Long, F. S. Bakrin, C. S. Tan, K. W. Goh, S. F. Yeoh, M. J. Loy, Z. Hussain, K. S. Lee, A. C. Idris, and L. C. Ming, "The use of blockchain technology in the health care sector: Systematic review," *JMIR Med. Informat.*, vol. 10, no. 1, Jan. 2022, Art. no. e17278.

[5] B. Panchal, S. Parmar, T. Rathod, N. Kumar Jadav, R. Gupta, and S. Tanwar, "AI and blockchain-based secure message exchange framework for medical Internet of Things," in *Proc. Int. Conf. Netw., Multimedia Inf. Technol. (NMITCON)*, Sep. 2023, pp. 1–6.

[6] K. Kumari and S. Yadav, "Linear regression analysis study," *J. Pract. Cardiovascular Sci.*, vol. 4, pp. 6–33, Jan. 2018.

[7] O. P. Olawale and S. Ebadinezhad, "The detection of abnormal behavior in healthcare IoT using IDS, CNN, and SVM," in *Mobile Computing and Sustainable Informatics*. Singapore: Springer, 2023.

[8] V. Jain and A. Dhruv, "Examining the influence of explainable artificial intelligence on healthcare diagnosis and decision making," in *Proc. 2nd Int. Conf. Advancement Comput. Comput. Technol. (InCACCT)*, May 2024, pp. 136–141.

[9] B. Sekeroglu, Y. K. Ever, K. Dimililer, and F. Al-Turjman, "Comparative evaluation and comprehensive analysis of machine learning models for regression problems," *Data Intell.*, vol. 4, no. 3, pp. 620–652, Jul. 2022.

[10] G. S. Ilgi, D. Kayali, P. Olawale, B. Demir Erdem, K. Dimililer, and Y. Kirsal-Ever, "Formal verification for security technologies in the blockchain with artificial intelligence: A survey," in *Proc. Innov. Intell. Syst. Appl. Conf. (ASYU)*, Sep. 2022, pp. 1–6.

[11] S. Mishra, "Blockchain and machine learning-based hybrid IDS to protect smart networks and preserve privacy," *Electronics*, vol. 12, no. 16, p. 3524, Aug. 2023.

[12] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review," *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023.

[13] S. V. N. S. Kumar, M. Selvi, and A. Kannan, "A comprehensive survey on machine learning-based intrusion detection systems for secure communication in Internet of Things," *Comput. Intell. Neurosci.*, vol. 2023, no. 1, pp. 1–24, Jan. 2023.

[14] M. Naveed, S. M. Usman, M. I. Satti, S. Aleshaiker, and A. Anwar, "Intrusion detection in smart IoT devices for people with disabilities," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Pafos, Cyprus, Sep. 2022, pp. 1–5.

[15] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[16] M. Abdullah, A. Alshannaq, A. Balamash, and S. Almabdy, "Enhanced intrusion detection system using feature selection method and ensemble learning algorithms," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 2, pp. 48–55, 2018.

[17] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. D. Hartog, "ToN_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 485–496, Jan. 2022.

[18] G. Zachos, G. Mantas, I. Essop, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, "Prototyping an anomaly-based intrusion detection system for Internet of Medical Things networks," in *Proc. IEEE 27th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Paris, France, Nov. 2022, pp. 179–183.

[19] R. Karim, M. A. I. Rizvi, and M. S. Arefin, "A survey on anomaly detection strategies," in *Proc. 2nd Int. Conf. Image Process. Capsule Netw. (ICIPCN)*, 2021, pp. 289–297.

[20] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, Jul. 2020.

[21] M. Islam, A. S. Dukyil, S. Alyahya, and S. Habib, "An IoT enable anomaly detection system for smart city surveillance," *Sensors*, vol. 23, no. 4, p. 2358, Feb. 2023.

[22] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1690–1700, Mar. 2014.

[23] M. Shahin, F. F. Chen, A. Hosseinzadeh, H. Bouzary, and R. Rashidifar, "A deep hybrid learning model for detection of cyber attacks in industrial IoT devices," *Int. J. Adv. Manuf. Technol.*, vol. 123, no. 5, pp. 1973–1983, 2022, doi: 10.1007/s10845-021-01856-2.

[24] B. Weinger, J. Kim, A. Sim, M. Nakashima, N. Moustafa, and K. J. Wu, "Enhancing IoT anomaly detection performance for federated learning," *Digit. Commun. Netw.*, vol. 8, no. 3, pp. 314–323, Jun. 2022.

[25] I. Tareq, B. M. Elbagoury, S. El-Regaily, and E.-S.-M. El-Horbaty, "Analysis of ToN-IoT, UNW-NB15, and edge-IIoT datasets using DL in cybersecurity for IoT," *Appl. Sci.*, vol. 12, no. 19, p. 9572, Sep. 2022.

[26] S. Latif, Z. E. Huma, S. S. Jamal, F. Ahmed, J. Ahmad, A. Zahid, K. Dashtipour, M. U. Aftab, M. Ahmad, and Q. H. Abbasi, "Intrusion detection framework for the Internet of Things using a dense random neural network," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6435–6444, Sep. 2022.

[27] G. Guo, "An intrusion detection system for the Internet of Things using machine learning models," in *Proc. 3rd Int. Conf. Big Data, Artif. Intell. Internet Things Eng. (ICBAIE)*, Jul. 2022, pp. 332–335.

[28] S. Kerrison, J. Jusak, and T. Huang, "Blockchain-enabled IoT for rural healthcare: hybrid-channel communication with digital twinning," *Electronics*, vol. 12, no. 9, p. 2128, May 2023.

[29] A. S. Rajasekaran, A. Maria, M. Rajagopal, and J. Lorincz, "Blockchain enabled anonymous privacy-preserving authentication scheme for Internet of Health Things," *Sensors*, vol. 23, no. 1, p. 240, Dec. 2022.

[30] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021.

[31] N. Kumar and A. Kundu, "Cyber security focused deepfake detection system using big data," *Social Netw. Comput. Sci.*, vol. 5, no. 6, p. 752, Aug. 2024.

[32] N. Kumar, A. Hashmi, M. Gupta, and A. Kundu, "Automatic diagnosis of COVID-19 related pneumonia from CXR and CT-scan images," *Eng., Technol. Appl. Sci. Res.*, vol. 12, no. 1, pp. 7993–7997, Feb. 2022.

[33] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 102994.

[34] N. Moustafa, M. Keshky, E. Debiez, and H. Janicke, "Federated TON_IoT windows datasets for evaluating AI-based security applications," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou, China, Dec. 2020, pp. 848–855.

[35] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022.

[36] U. C. Akuthota and L. Bhargava, "Evaluation of machine learning models for intrusion detection with the UNSW-NB15 dataset," in *Proc. IEEE Silchar Subsection Conf. (SILCON)*, Nov. 2023, pp. 1–5.

[37] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.

[38] M. Chen, Q. Liu, S. Chen, Y. Liu, C.-H. Zhang, and R. Liu, "XGBoost-based algorithm interpretation and application on post-fault transient stability status prediction of power system," *IEEE Access*, vol. 7, pp. 13149–13158, 2019.

[39] A. Sharma, A. Tyagi, and M. Bhardwaj, "Analysis of techniques and attacking pattern in cyber security approach: A survey," *Int. J. Health Sci.*, vol. 6, pp. 13779–13798, Jun. 2022.

[40] S. He, J. Fu, C. Chen, and Z. Guo, "Research on password cracking technology based on improved transformer," *J. Phys., Conf. Ser.*, vol. 1631, no. 1, 2020, Art. no. 012161.

[41] S. J. Y. Weamie, "Cross-site scripting attacks and defensive techniques: A comprehensive survey," *Int. J. Commun., Netw. Syst. Sci.*, vol. 15, no. 8, pp. 126–148, 2022.

[42] T. Al Nuaimi, S. Al Zaabi, M. Alyilieli, M. AlMaskari, S. Alblooshi, F. Alhabsi, M. F. B. Yusof, and A. Al Badawi, "A comparative evaluation of intrusion detection systems on the edge-IIoT-2022 dataset," *Intell. Syst. With Appl.*, vol. 20, Nov. 2023, Art. no. 200298.

[43] N. Singh and P. Singh, "Exploring the effect of normalization on medical data classification," in *Proc. Int. Conf. Artif. Intell. Mach. Vis. (AIMV)*, Sep. 2021, pp. 1–5.

[44] I. Izonin, B. Ilchyshyn, R. Tkachenko, M. Greguš, N. Shakhovska, and C. Strauss, "Towards data normalization task for the efficient mining of medical data," in *Proc. 12th Int. Conf. Adv. Comput. Inf. Technol. (ACIT)*, Sep. 2022, pp. 480–484.

[45] S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj and D. J. Inman, "1D convolutional neural networks and applications: A survey," *Mech. Syst. Signal Process.*, vol. 157, Apr. 2021, Art. no. 107398.

[46] O. P. Olawale and K. Dimililer, "Individual eye gaze prediction with the effect of image enhancement using deep neural networks," in *Proc. 4th Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT)*, Oct. 2020, pp. 1–7.

[47] O. P. Olawale, F. Ozdamli, and K. Dimililer, "Data mining techniques for the classification of medical cases: A survey," in *Proc. 5th Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT)*, Oct. 2021, pp. 68–73.

[48] N. Cristianini and E. Ricci, "Support vector machines," *Encyclopedia Algorithms*, vol. 58, pp. 928–932, Sep. 2008.

[49] A. M. Said, A. Yahyaoui, and T. Abdellatif, "Efficient anomaly detection for smart hospital IoT systems," *Sensors*, vol. 21, no. 4, p. 1026, Feb. 2021.

[50] Y. Y. Song and Y. Lu, "Decision tree methods: Applications for classification and prediction," *Shanghai Arch. Psychiatry*, vol. 27, no. 2, pp. 130–135, Apr. 2015.

[51] J. H. Friedman, "Greedy function approximation: A gradient boosting machine.," *Ann. Statist.*, vol. 29, no. 5, pp. 1189–1232, Oct. 2001.

[52] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, pp. 5–32, Oct. 2001.

[53] M. G. Ismail, M. A. E. Ghany, and M. A.-M. Salem, "Enhanced recursive feature elimination for IoT intrusion detection systems," in *Proc. Int. Conf. Microelectron. (ICM)*, Casablanca, Morocco, Dec. 2022, pp. 193–196.

[54] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.

[55] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for blockchain-based IoT systems: A review," *Appl. Sci.*, vol. 13, no. 13, p. 7432, Jun. 2023.

[56] N. R. Chandran and E. M. Manuel, "Performance analysis of modified SHA-3," *Proc. Technol.*, vol. 24, pp. 904–910, Jan. 2016.

[57] F. Laiq, F. Al-Obeidat, A. Amin, and F. Moreira, "DDoS attack detection in edge-IIoT using ensemble learning," in *Proc. 7th Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2023, pp. 204–207.

[58] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly detection in 6G networks using machine learning methods," *Electronics*, vol. 12, no. 15, p. 3300, Jul. 2023.

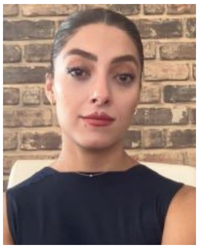
[59] A. Roy and K. J. Singh, "Multi-classification of UNSW-NB15 dataset for network anomaly detection system," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 15, pp. 429–451, 2020.

[60] R. Abiyev, M. Arslan, J. Bush Idoko, B. Sekeroglu, and A. Ilhan, "Identification of epileptic EEG signals using convolutional neural networks," *Appl. Sci.*, vol. 10, no. 12, p. 4089, Jun. 2020.

[61] T. R. Xuan and S. Ness, "Integration of blockchain and AI: Exploring application in the digital business," *J. Eng. Res. Rep.*, vol. 25, no. 8, pp. 20–39, Aug. 2023.

[62] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the integration of artificial intelligence and blockchain technology: A perspective about security," *IEEE Access*, vol. 12, pp. 3881–3897, 2024.

OLUWASEUN PRISCILLA OLAWALE received the bachelor's degree in computer science from Bowen University, Nigeria, in 2016, and the master's degree in software engineering from Near East University, in 2020. She is currently a Lecturer with the Department of Software Engineering and Artificial Intelligence Engineering, Near East University. She has authored several publications indexed in Scopus and Web of Science. Her research interest includes medical information technology.



SAHAR EBADINEZHAD received the M.S. degree in computer engineering from Eastern Mediterranean University (EMU), Cyprus, in 2014, and the Ph.D. degree in computer engineering from Cyprus International University (CIU), Cyprus. Her dedication to academia and research led her to join the Department of Computer Information Systems, University of Near East, in 2017, where she is currently a full-time Lecturer. She is an accomplished scholar and an educator in the field of computer engineering. As a Distinguished Member with the Computer Information Systems Research and Technology Center (CISRTC), Near East University, she has been at the forefront of cutting-edge research in the field. Her extensive body of work includes numerous publications in her areas of expertise. Her research interests include wireless communications systems, millimeter wave communication, vehicular communication (V2X), body-centric communications, wearable communication, artificial intelligence, the IoT, and cloud computing. Her contributions to the academic and research community have established her as a respected authority in the field of computer engineering. Her work continues to drive innovation and advance the boundaries of knowledge in wireless communication technologies.