IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 14, 2021, accepted November 7, 2021, date of publication November 16, 2021,
date of current version December 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3128837

Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms

YAKUB KAYODE SAHEED[1,2], (Member, IEEE), AND MICHEAL OLAOLU AROWOLO[3,4], (Member, IEEE)

[1]School of IT and Computing, American University of Nigeria, Yola 640101, Nigeria
[2]Kaptain A. I & Innovation Research Group
[3]Department of Computer Science, Landmark University, Omu-Aran 251103, Nigeria
[4]Industry, Innovation, and Infrastructure Research Group, Landmark University SDG9, Nigeria

Corresponding author: Yakub Kayode Saheed (yakubu.saheed@aun.edu.ng)

This work was supported by the Landmark University, Omu-Aran, Kwara State, Nigeria.

ABSTRACT Information and communication technology (ICT) advancements have altered the entire computing paradigm. As a result of these improvements, numerous new channels of communication are being created, one of which is the Internet of Things (IoT). The IoT has recently emerged as cutting-edge technology for creating smart environments. The Internet of Medical Things (IoMT) is a subset of the IoT, in which medical equipment exchange information with each other to exchange sensitive information. These developments enable the healthcare business to maintain a higher level of touch and care for its patients. Security is seen as a significant challenge in whatsoever technology's reliance based on the IoT. Security difficulties occur owing to the various potential attacks posed by attackers. There are numerous security concerns, such as remote hijacking, impersonation, denial of service attacks, password guessing, and man-in-the-middle. In the event of such attacks, critical data associated with IoT connectivity may be revealed, altered, or even rendered inaccessible to authorized users. As a result, it turns out to be critical to safeguard the IoT/IoMT ecosystem against malware assaults. The main goal of this study is to demonstrate how a deep recurrent neural network (DRNN) and supervised machine learning models (random forest, decision tree, KNN, and ridge classifier) can be utilized to develop an efficient and effective IDS in the IoMT environment for classifying and forecasting unexpected cyber threats. Preprocessing and normalization of network data are performed. Following that, we optimized features using a bio-inspired particle swarm algorithm. On the standard data for intrusion detection, a thorough evaluation of experiments in DRNN and other SML is performed. It was established through rigorous testing that the proposed SML model outperforms existing approaches with an accuracy of 99.76%.

INDEX TERMS Internet of Medical Things, cyber-attack, Internet of Things, particle swarm optimization, recurrent neural network, smart environment.

I. INTRODUCTION

The Internet of Things (IoT) is a type of network that connects anything to the Internet via a specific protocol and data sensing devices, enabling data sharing and exchanges and enabling intelligent identification, tracking, placement, monitoring, and administration [1]. The IoT is frequently described as a network of real objects. However, the internet has progressed into a network of devices of various types and sizes, including smartphones, home appliances, vehicles, cameras, toys, medicinal tools, people, technological frameworks, structures, and animals, all of which are connected and share data according to predefined protocols [2]. The IoT goal is to make it possible for things to be connected at any moment, everywhere, with anybody and anything, preferably over any network and with any support [2].

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

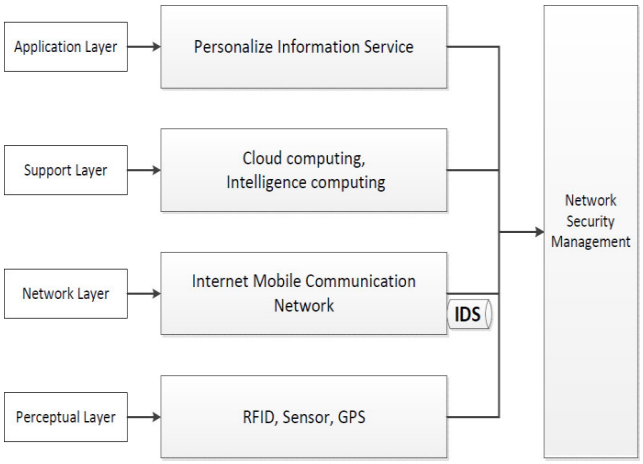

FIGURE 1. Framework of IoT [5].

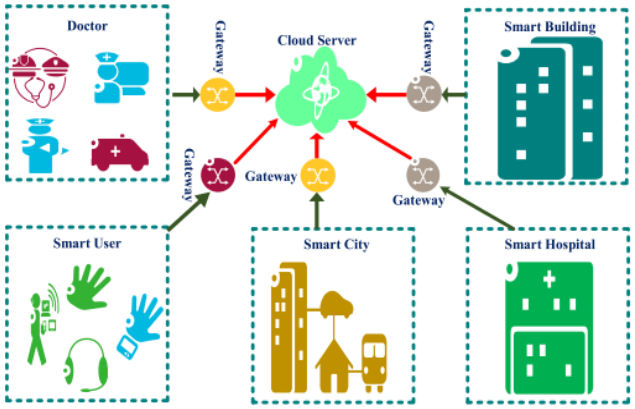

FIGURE 2. IoMT architecture [9].

The IoT offers a plethora of uses. Smart health services, smart grids, and smart transportation, and constructions are all well-known uses [3]. Figure 1 depicts the IoT's four-layer design. In addition, the IoT is a new paradigm in which a network of real items equipped with sensors aims to combine the digital and physical worlds seamlessly. The IoT revolution, fueled in large part by advancements in sensor networks, wireless communications, cloud computing, and mobile devices, is reimagining modern healthcare and altering its reliability and delivery [4].

The Internet of Medical Things (IoMT) is a recent development that is a component of the IoT. It is an environment in which numerous healthcare gadgets such as smart glucometers, smart blood pressure displays, smart bands, Intelligent pacemakers, and Intelligent pulse rate monitors are linked and interact with one another to distribute sensitive medical information that is used by health care officials, hospitals, and doctors to provide exceptional medication and support [6]–[8]. These confidential data are kept on some data centers by the gateway and then sent to the appropriate end users [9]. IoMT architecture is depicted in Figure 2, which connects various medical smart appliances and interacts with clinicians to provide effective treatment and assistance. The data is hosted in the cloud, and distributed to end-users via a separate gateway. Remote patient monitoring has been expanded with the advent of the IoMT. By linking outpatients to their doctors and permitting for the secure transfer of health information via a protected web, it helps reduce needless hospital visits and the stress on systems of health care. At the moment, this is fundamentally important owing to the worldwide pandemic, COVID-19, which is limiting in-person medical appointments, thereby preventing the spread.

In addition, the IoMT was born as a result of the incorporation of medical equipment into the IoT [10]. With the advent of the modern digitized healthcare age dubbed Healthcare vs4.0 [11], [1], IoT equipment's have been used in a variety of medical domains, most notably through the widespread use of medical wearable sensors, gadgets, robots, and unmanned aerial vehicles (UAVs). Indeed, in the context of body area networks, actuators and medical sensors are utilized as wearable gadgets. Rather than confining patients in hospitals, these technologies are capable of monitoring their health in real-time and improving their physical mobility and flexibility. On either hand, medical robots can also be used as hospital robots and surgical robots [1], capable of performing minor surgery accurately. Additionally, they can perform a variety of surgical treatments, including cardiopulmonary resuscitation (CPR) [12]. Nevertheless, the central problem is that several IoMT devices are susceptible to and prone to cyber-attacks merely because medical equipment is either inadequately guarded against prospective attackers or is completely insecure. As a result, any cyber-attack might have dire effects, endangering patients' lives and impeding the widespread adoption of IoMT. Hackers are also motivated by the growth and developments in technology to break into the servers that house this sensitive data. Numerous attack vectors might be exploited to take control of these intelligent medical accessories. For instance, if an intruder takes possession of intelligent pacemakers, he'll be able to take the patient by surprise, perhaps resulting in death. These emergent risks have the potential to negatively impact the IoMT ecosystem and so must be addressed immediately [13].

It is not only the IoMT transforming the healthcare industry, but it is also facilitating a more humane approach to patient healing and care. It is, nevertheless, vulnerable to a variety of cyber-attacks and susceptibilities. The authors [14] identified several causes for the high number of cyber-attacks in IoMT, including the following: (1) Compatibility and complexity issues that arise when a large number of gadgets and diverse networks are connected. (2) Medical Things is largely concerned with the exchange of delicate patient data. (3) As a burgeoning paradigm, there is the rapid adoption of IoMT solutions by healthcare makers without regard for security concerns. As a consequence, additional concerns about confidentiality, integrity, and availability (CIA) emerge. (4) Application risks, such as authorization and authentication breaches, are likewise a big concern, as is the application's general security and availability. (5) Certain security computations need a sizable

proportion of computing powers. (6) Because the majority of IoT components receive and transmit data wirelessly, IoMT is at risk of WSN security violations. These are only a few of the primary reasons why IoMTs are vulnerable to a variety of harmful assaults.

Most of these linked appliances are unsecured, and the possible influence is not just on patients' records, but also on outpatient care, as any mistake in a patient's document or analysis could result in their death. As a result, it is critical to address how to recognize and guard against medical equipment assaults. While the majority of IoT vulnerabilities also apply to IoMTs, although, some are much more specifically pointed at IoMTs because of the delicate essence of healthcare data. These assaults comprise, but are not restricted to, data breaches, man-in-the-middle assaults, probe attacks, decryption of network communication, DoS attack, and privacy and security issues.

According to an IBM survey, healthcare firms incurred the largest losses as a result of data theft [15].

Additionally, Help Net security reports that hackers infiltrated Singapore's health system, stealing private information from 1.5 million patients and compromising outpatient prescription data for 160,000 persons, which include Singapore's Prime Minister [16]. The health sector is perpetually beset by a slew of cybersecurity-related problems. These concerns vary from ransomware that undermines system integrity and patient privacy to DDoS assaults that impair institutions' capacity to deliver outpatient care. Secure transmission of delicate data, akin to protected health info, across the IoMT, in addition to continuous access to the computer system, is growing anxiety for healthcare practitioners. While other vital groundwork industries are often targeted, the healthcare sector has specific hurdles due to the nature of its mission. It extends beyond monetary loss and invasion of privacy to have a direct effect on human existence. Regardless of the motivation for an attack on the healthcare system, great or minor, they continue to constitute a threat. As IoMT grow ingrained in hospital, we must devise a strategy for their secure and effective management.

Conventional information technology security measures do not take into account the setting of connected medical equipment. Security research in this domain is now focusing on the implementation of encryption, authentication, and trust-based systems for implantable, and wearable medical products [17]–[19]. These cryptographic solutions are frequently computationally intensive and difficult to apply on a limited resource medical equipment [4]. Physical layer safety has lately been considered as a promising substitute to cryptography, leveraging the physical layer characteristics of the net system to enhance the safety of IoT devices [20]. The major drawback of conventional information technology security measures such as encryption, authentication, and trust-based system is that they are difficult to apply and cannot guarantee adequate security. Therefore, the second line of defense is needed. However, before physical layer security solutions are used by practical systems, issues like weak attacker models regarding wireless channels must be addressed [21].

The proposed method for detecting assaults in the IoMT includes the different attacks such as DoS, Brute force, and botnet are all examples of attacks in this data that might result in the disappointment of an IoT system. In this study, we take a different approach to cryptographic security solutions and present detection of intrusion solutions grounded on ML and DL for detecting cyber-attacks in IoMT. While there is extensive research on utilizing cryptography to detect IoMT assaults, research on intrusion detection in IoMT is still in its infancy, and to the best of our knowledge, there is no research on using wrapper-based PSO feature selection to improve IDS performance in IoMT. This paper is organized as follows. Section 2 discusses the related work. Section 3 presents the proposed methodology. Section 4 reports the results and discussion. Section 5 concludes the paper.

II. RELATED WORK

This section covers work in the relevant area of IDS.

Because patient data is sensitive and confidential, privacy and security are crucial in IoMT applications. Numerous academics have conducted surveys on the topic of offering privacy, confidentiality, and safety solutions in IoMT [23].

The authors [5] provided an IDS for the detection of various threats such as DoS, Botnet, and web attacks in IoMT contexts. The CICIDS dataset was used to conduct the experiment, which used the DBN model to spot these assaults. The botnet attack had an accuracy of 97.93 percent. The authors overlook the feature selection phase, which was identified as a fundamental flaw in IDS in the IoMT environment.

The authors of [24] presented a framework for IoMT applications, data gathering, and analysis that is privacy-preserving. On the NSL-KDD datasets, FFDNN is combined with the FBFSA to detect anomaly incursion in wireless networks. For wireless networks, the algorithm picks the best feature with the least amount of redundancy. It is composed of three deep layers and contains a soiree of 30 neurons. The data is separated into training and testing segments in this article, resulting in a 99.69 percent accuracy [25].

Thamilarasu et al [4] design a new IDS based on mobile agents to safeguard a network of linked medical equipment. The suggested system, in particular, is layered, autonomous, and utilizes ML and regression methods to detect network-level attacks and also abnormalities in wearable sensors. They replicated a hospital network and conducted comprehensive experiments on a variety of IoMT subsets, such as wireless body area networks as well as other linked medical instruments. The authors of [26] suggested a two-stage DL method that utilizes a soft-max technique and stacked autoencoder for ID. The suggested system is made up of three layers: input, concealed, and output. The likelihood score model was employed in the first stage to classify network circulation as regular or anomalous. The second phase used a soft-max to classify the data as regular, type 1, and type 2 attacks, and

so on. To demonstrate its efficiency, studies were conducted on two publicly available datasets, KDD'99 and the UNSW-NB15, which attained an accuracy reaching 99.99 percent and 89.13 percent, respectively. Asmae *et al.* [27] presented an IDS based on network metrics for detecting WBAN jamming attacks.

The authors of [28] detected infiltration in the system by combining an enhanced conditional variation autoencoder with a DNN. In DNN hidden layers, the ICAVE encoder conducts weight initialization. DNN is simple and quick to use because it reduces the dimensionality of features. The authors of [29] propose a methodology called deep adversary learning (DAL) that uses statistical learning and data enrichment to identify network infiltration. In data augmentation, this strategy solves the difficulties of data shortages and imbalances. The classifier is being used to reject intrusion enhanced data, while the producer is being used to generate intrusion enhanced datasets. SVM is being used to distinguish between normal and attack intrusion datasets. The experimentation was performed on the KDD Cup 99 data, and the findings revealed that when compared to conventional techniques, the precision, recall, and accuracy scores were improved. The researchers introduced a framework for cyber ID based on DBN and IGA in [30], which was primarily assessed on NSL-KDD datasets and showed a 99 percent detection accuracy rate. For intrusion detection, DBN employs IGA-generated optimum system features. However, training the dataset takes more time.

In reference [31], the researchers compared an IoT extracting features model with a predictive analysis system to create a cybersecurity IDS for smart cities using deep migrating supervised learning. The four steps of the deep migrating learning model are an ideal feature, variable, feature sampling, and knowledge. The KDD CUP 99 incursion dataset was used for this study's experiments conducted, which included 10,000 training data sessions at random and produced outcomes with the rate of detection 91.05 percent. Nevertheless, the intrusion detection rate performance can be enhanced further. The authors of [32] presented an RBM model having five (5) levels for detecting DDoS assaults in datasets from smart city applications. For pre-sample selection, an FFN is employed; for data classification, an RF and an SVM are utilized. RBM is used to process the K-means approach to learn critical features for sub-form datasets. In [33], GDM and GDM/AG are combined with a DLNN architecture to increase the accuracy and identification of automotive security intrusions. The suggested solution is validated using the Intelligent car CAN bus via the Kvasercan leaf version 2 device.

In [34], a novel hybrid model based on IG and PCA was introduced to spot intrusion on the NSL-KDD, the Kyoto 2006+ and ISCX 2012datasets using an MLP, IBK, and SVM. The KDD99 dataset is used in [35] to identify anomalous cyber intrusion threats using a SoftMax algorithm and CNN. The authors employed 494021 samples for training and 311029 sample for testing, achieving a 99.23 percent accuracy rate. The summary of other existing methods is given in Table 1.

TABLE 1. Existing methods performance.

Authors	Method	Findings	Limitations
Nguyen et al., [36]	CNN	Accuracy: 92.0; F1: 94	There is still room for improvement in terms of accuracy.
Kumar et al.,[37]	Blockchain and ML	Accuracy: 98.0; F1:98	The detection accuracy can yet be improved.
Su et al.,[38]	LCNN	Accuracy: 94.0	No consideration was given to precision, MCC, or F1 metrics.
Dinnakaro et al.,[39]	HaRM	Accuracy: 92.21	Accuracy alone cannot ensure the effectiveness of IoMT detection.

III. METHODOLOGY

This section examines several methods and algorithms for categorizing attack occurrences in the IoMT environment. A comprehensive overview of the pre-processing phase, feature selection using swarm intelligence method recognized as the particle swarm optimization (PSO), and classification using SVM, RF, NB, and RNN.

A. PROPOSED APPROACH

The IoMT ecosystem is comprised of a variety of sensors that monitor patients' health and send periodic updates to clinicians who can maintain proximity. These devices are intelligent enough to gather subtle data and send it to a storing location such as a server in the cloud, they are not intelligent sufficient to determine if the data is being conveyed safely or whether any assailants have infringed before and during storage while interacting with the physician in the clinic. When an IoMT environment is used, numerous types of attacks are feasible, and our model focuses on detecting the probe, remote to local, user to root, and DoS attack. As seen in figure 3, data travels from medical various sensors to the body of the patient through the multispectral board, gateway, router, and finally to the servers and other observing equipment for viewing. Whereas the data is being transmitted from either the gateway via servers, an eavesdropper may change the therapeutic information in transit or perform DoS

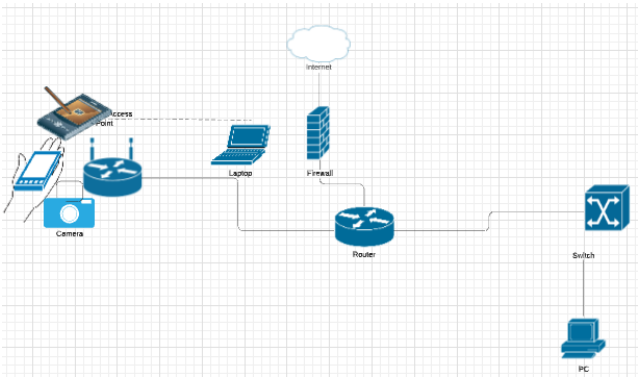

FIGURE 3. The architecture of the proposed IoMT-Smart environment.

attacks to prevent the information from accessing the display phase.

B. DATA FILTERING

The filtered data assists the system in presenting correctly structured data. The data was processed by transforming string attributes to numeric variables and removing inconsistencies [40], [41]. During this phase, an inconsistent element is also eliminated.

C. FEATURE SELECTION

Feature Selection (FS) is a method for picking and deleting a subset of relevant traits of many superfluous and repeated information from [42] the data to create efficient learning methods. FS can be defined as the process of removing redundant and irrelevant attributes from a dataset to enhance training achievement in terms of detection accuracy, and model construction time [43]. Apart from replica complexity, feature selection can assist in removing certain computations [44]. Process for Feature Selection: FS techniques follow a four-stage process, as illustrated in Figure 4. In this research, the PSO is utilized for FS to select twenty-one (21) attributes out of the forty attributes (40) with one class from the NSL-KDD dataset.

1. The sequence of production processes for the future applicant subgroup
2. Its estimation function is capable of estimating the subgroup.
3. Criteria for determining when to terminate
4. The acceptance procedure is used to validate the subgroup.

D. PARTICLE SWARM OPTIMIZATION

In the year 1995, Eberhart and Kennedy presented a method of optimization called PSO, which was enthused by animal behavior [45]. A swarm of particles continuously explores the search area for a problem to determine the global best configuration [46]. Ever since its conception in 1995, PSO has been used to a growing number of complicated, real-world optimization issues where standard methods either underperform or have limited utility [47]. Its visually simple

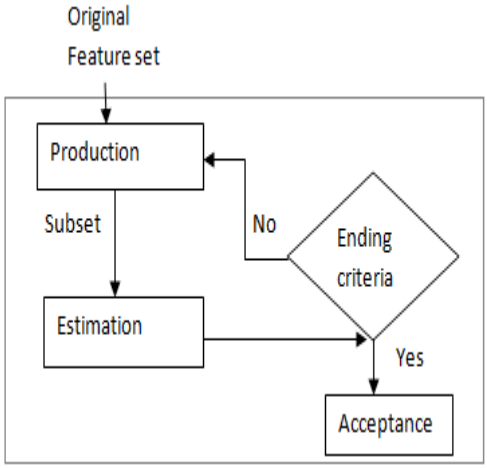

FIGURE 4. Main FS steps [42].

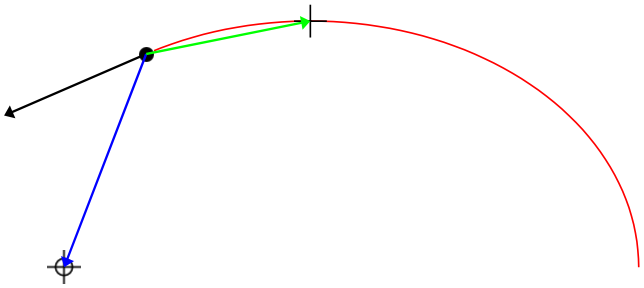

FIGURE 5. These are the three forces that act on PSO particles [48].

form and very few adjustable parameters make it perfect for a wide variety of issues that require approximation to some degree. The PSO was adopted to select the significant features of the attacks in the dataset. We used PSO which is a metaheuristic optimization algorithm for FS to select the most relevant attributes in the NSLKDD data before we now subject the features to classification.

E. ASSUMPTION OF THE PSO

In PSO, each particle i's position xi denotes a potential solution to the issue, with fitness f(xi). The particles travel as a factor of the velocity vi during each round of the search method. Thus, the searching space's structure must facilitate such mobility. For instance, finding the optimal value of a linear combination in Rn enables this. The movement of the particles is comparable to that of a flock of birds, a school of fish, or a swarm of insects. In these scenarios, it is believed that the creatures follow the group member who is aware of the optimal path, which may be a food source. As demonstrated in Figure 5, three factors determine the particle movement in PSO. To begin, there is a term that accounts for the particles' ''inertia'': this term tends to retain them on their current track. Second, they are drawn to Z(p), the world's best. Thirdly, they are drawn to their fittest point j greatest i (p).

The trajectory of the particle is indicated in red; its current motion is indicated in blue; the pull towards to the global-best

is indicated in green; and the attractiveness toward the particle-best is indicated in green. The following formulas control the relationship of a particles from one cycle to the next mathematically [48]:

$$k_i(p+1) = wk_i(p) + b_1q_1(p+1)[j_i^{best}(p) - j_i(p)] + b_2\, q_2(p+1)[Z(p) - j_i\,(p)] \quad (1)$$

$$j_i(p+1) = j_i(p) + k_i(p) + k_i(p+1) \quad (2)$$

where, w, b1 and b2 are defined constants, and q1 and q2 are pseudo-random values distributed uniformly in the range [0, 1].

F. RECURRENT NEURAL NETWORK

RNN, which is a variant of a feed-forward neural network, tends to make use of sequential data. The term ''recurrent neural networks'' refers to the fact that they perform the same task for each component of categorization, with the outcome dependent on the preceding computation [49]. Because RNNs include cyclic connections, they are particularly well-suited for simulating sequences [50].

G. RANDOM FOREST

RF is a group learning method that is used to increase the accuracy of classifications [51]. An RF is made up of several decision trees. In comparison to other classic classification techniques, RF has a low classification error. The RF produces a large number of categorization trees. The tree is generated using a tree classification method and separate bootstrap samples from the original data [52]. Just after a forest is established, each tree inside the forest is assigned a new item that must be classified. Random Forest creates every tree using a unique sample from the original data and a tree classification method [53].

H. DECISION TREE

DT is a non-linear and non-parametric data mining technique that is used for regression learning and supervised classification [54]. This is a household of algorithms for supervised learning. The DT principles are simple to comprehend for the user when combined with a knowledge management system [55]. The primary goal of their DT rule is to generate a training model from which the projected label rate is derived [46]. The structure of a decision tree is characterized as a tree; the tree has decision nodes and leaf nodes [56]. It is the origin node, with each interior node representing a feature.

I. K NEAREST NEIGHBOR

By comparing the test record with the training record that has similarities, the classification employs the k-NN algorithm based on analogy [57]. Classification is performed using the k-NN method based on similarity, by matching the test record to the similar training record. It compares the unlabeled data to the training instances [58]. The training dataset are matrices in a multidimensional space; each trial has a class name associated with it. k is a user-defined constant variable in the classification phase, and an unidentified vector is discriminated by conveying the class that is most frequently occurring amongst some of the k training instances closest to the query instance [59]. Euclidean distance is a frequently used distance metric. Assume that two variables $Y = (y_1, y_2, y_3, \ldots y_n)$ and $Z = (z_1, z_2, z_3 \ldots z_n)$. Euclidean distance is defined as:

$$d\,(Y, Z) = \sqrt{(y1 - z1)}^2\,(y_2 - z_2)^2 + \ldots + (y_3 - z_3) \quad (3)$$

TABLE 2. Classification Performance of PSO-RNN model.

Technique	Accuracy	Recall	Precision	MCC
PSO-RNN	96.08	85.63	85.63	98.15

J. RIDGE CLASSIFIER

The RC is based on a linear model, in which the parameter matrix is used to reflect the coefficients of a linear model, with the components of the characteristic vector x representing the factors [60].

IV. RESULTS AND DISCUSSION

As can be seen in the related work constraints, In terms of accuracy, there is still space for improvement, detection accuracy may still be increased, and precision, MCC, and F1-measures were not taken into account. This study addressed the literature's limitations.

A. PERFORMANCE MEASURES

Accuracy: The model's accuracy was assessed based on a subset of the model's performance. The accuracy estimation is represented by equation (4).

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

Recall: The total positives in the scheme states versus the precise total of positives in the data is referred to as the recall or TP value, which denotes the total positives in the classification states versus the actual total of positives in the data. In equation 5, the recall rate is shown.

$$\frac{TP}{(TP + FP)} \quad (5)$$

F1-Score: Model performance could also be estimated using the F1 score. It's the model's weighted average of recall and precision. The F1 Score's value is given in equation (6).

$$\frac{2{*}TP}{2{*}TP + FP + FN} \quad (6)$$

B. EXPERIMENTAL ANALYSIS OF THE DEEP RECURRENT NEURAL NETWORK

As can be seen in Table 2, the PSO-RNN gave an accuracy of 96.08%, recall of 85.63%, precision of 85.63%, and MCC of 98.15.

TABLE 3. Classification Performance of the proposed models.

Proposed Approaches	Accuracy	Recall	Precision	MCC
PSO-RF	99.76	96.45	99.75	99.51
PSO-DT	99.58	96.27	99.59	99.15
PSO-KNN	98.90	92.33	98.89	97.77
PSO-RC	97.61	91.06	97.60	95.14

TABLE 4. The training time of RF, DT, KNN, and RC.

Propose Approaches	Training Time (seconds)
PSO-RF	0.1181
PSO-DT	0.0511
PSO-KNN	0.1052
PSO-RC	0.0432

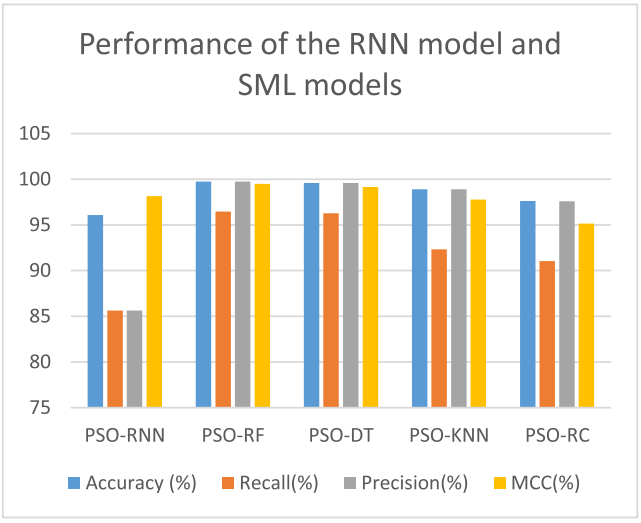

FIGURE 6. Classification Performance of SML models and RNN model.

C. EXPERIMENTAL ANALYSIS OF THE PROPOSE PSO-RF, PSO-DT, PSO-KNN, AND PSO-RC

The performance of the proposed SML techniques is revealed in this section as seen in Table 3. The PSO-RF gave an accuracy of 99.76%, recall of 96.45%, precision of 99.75%, and MCC of 99.51%. The PSO-DT gave an accuracy of 99.58%, recall of 96.27%, precision of 99.59%, and MCC of 99.15%. The PSO-KNN revealed an accuracy of 98.90%, recall of 92.33%, precision of 98.89%, and MCC of 97.77%. The PSO-RC revealed an accuracy of 97.61%, recall of 91.06%, precision of 97.60%, and MCC of 95.14%.

D. TRAINING TIME OF THE SUPERVISED MACHINE LEARNING MODELS

As seen in Table 4, the training time of the RF model gave 0.1181 seconds, DT revealed 0.0511 seconds, KNN gave 0.1052 seconds and RC yielded 0.0432 seconds.

The performance of the proposed RNN model and the SML models: RF, DT, KNN, and RC is given in Figure 6.

TABLE 5. Comparison with the previous models.

Authors	Method	Accuracy	F1	Precision	MCC
Ref.[36]	CNN	92.0	94	NA	NA
Ref. [37]	Block chain and ML	98.0	98	NA	NA
Ref.[38]	LCNN	94.0	NA	NA	NA
Ref. [39]	HaRM	92.21	NA	NA	NA
Propose d model	**PSO-RF**	**99.76**	**96.45**	**99.75**	**99.51**

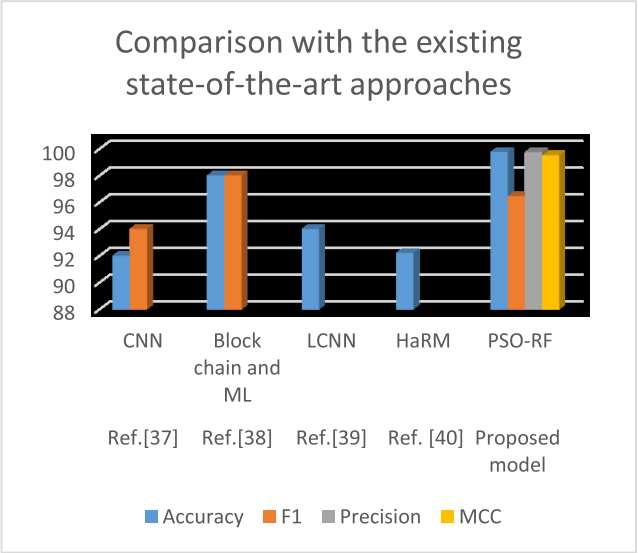

FIGURE 7. Comparison with the state-of-the-art methods.

The proposed SML models outperformed the RNN model in terms of accuracy, recall, precision, and MCC.

E. COMPARISON WITH THE EXISTING APPROACHES

We compare the performance of the existing system with our proposed models in this section as shown in Table 5. The author's reference [36] method achieve an accuracy of 92% and F1 of 94%. Reference [37] achieves an accuracy of 98% and F1 of 98%. The authors [38] achieve an accuracy of 94%. While the authors [39] revealed an accuracy of 92.21%. The proposed model achieves an accuracy of 99.76%, F1 of 96.45%, the precision of 99.75%, and MCC of 99.51%.

The comparison with the state-of-the-art approaches is illustrated in Figure 7, the proposed model PSO-RF achieves the best accuracy, precision, and MCC at the expense of the F1. The existing methods outperformed our model in terms of F1.

V. CONCLUSION

The study offers a classification model based on RNN and SML for identifying intruder assaults using the benchmarked NSLKDD datasets, which include DoS attacks, probing

attacks, u2R attacks, and remote to local assault in the IoMT environment. The suggested technique may be most appropriate for IoMT environments in which smart medical appliances can communicate with one another using peer-to-peer different internet protocol addresses. The resampled data set is then subsequently lowered utilizing PSO to decrease attribute dimension and to identify the most influential features. Following that, the reduced data set is categorized using a variety of state-of-the-art ML algorithms, including RF, DT, KNN, RC, and RNN. Our model's accuracy achieved competitive results and also indicated a decrease within the time frame required to train the classifiers, which is the finest suitable for IoMT architecture, resulting in faster notifications to health - care authorities whenever an assault occurs in their ecosystem. The future work will be on evaluating the effectiveness of the proposed system for detecting IoMT attacks using blockchain technology.

REFERENCES

[1] J. Rosen and B. Hannaford, "Doc at a distance," *IEEE Spectr.*, vol. 43, no. 10, pp. 34–39, Oct. 2006.

[2] K. K. Patel and S. M. Patel, "Internet of things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, 2016.

[3] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2988293.

[4] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020, doi: 10.1109/ACCESS.2020.3026260.

[5] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020, doi: 10.1109/ACCESS.2020.2986013.

[6] I. Lokshina and C. Lanting, "A qualitative evaluation of IoT-driven eHealth: Knowledge management, business models and opportunities, deployment and evolution," in *Data-Centric Business and Applications* (Lecture Notes on Data Engineering and Communications Technologies), vol. 20, N. Kryvinska and M. Greguš, Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-319-94117-2_2.

[7] E. K. Wang, C.-M. Chen, M. M. Hassan, and A. Almogren, "A deep learning based medical image segmentation technique in Internet-of-Medical-Things domain," *Future Gener. Comput. Syst.*, vol. 108, pp. 135–144, Jul. 2020, doi: 10.1016/j.future.2020.02.054.

[8] M. Sikarndar, W. Anwar, A. Almogren, I. U. Din, and N. Guizani, "IoMT-based association rule mining for the prediction of human protein complexes," *IEEE Access*, vol. 8, pp. 6226–6237, 2020, doi: 10.1109/ACCESS.2019.2963797.

[9] S. P. Rm, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020, doi: 10.1016/j.comcom.2020.05.048.

[10] E. Balandina, S. Balandin, Y. Koucheryavy, and D. Mouromtsev, "IoT use cases in healthcare and tourism," in *Proc. IEEE 17th Conf. Bus. Informat.*, Jul. 2015, pp. 37–44, doi: 10.1109/CBI.2015.16.

[11] Z. Pang, G. Yang, R. Khedri, and Y. Zhang, "Introduction to the special section: Convergence of automation technology, biomedical engineering, and health informatics toward the healthcare 4.0," *IEEE Rev. Biomed. Eng.*, vol. 11, pp. 249–259, 2018, doi: 10.1109/RBME.2018.2848518.

[12] R. A. Beasley, "Medical robots: Current systems and research directions," *J. Robot.*, vol. 2012, pp. 1–14, Oct. 2012, doi: 10.1155/2012/401613.

[13] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.

[14] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120, doi: 10.1109/LCN.Workshops.2017.72.

[15] *Criminals and Hostile States Attack Healthcare With Impunity; the CyberPeace Institute Calls for Accountability*, CyberPeace Inst., Geneva, Switzerland, Mar. 2021.

[16] T. Haukilehto, "Masters—Improving cyber security awareness," BBC, Asia, Tech. Rep., Apr. 2019.

[17] R. V. Sampangi, "A security suite for wireless body area networks," *Int. J. Netw. Secur. Appl.*, vol. 4, no. 1, pp. 97–116, Jan. 2012, doi: 10.5121/ijnsa.2012.4110.

[18] A. S. Sangari and J. M. L. Manickam, "Public key cryptosystem based security in wireless body area network," in *Proc. Int. Conf. Circuits, Power Comput. Technol. (ICCPCT)*, Mar. 2014, pp. 1609–1612, doi: 10.1109/ICCPCT.2014.7054788.

[19] W. Li and X. Zhu, "Recommendation-based trust management in body area networks for mobile healthcare," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2014, pp. 515–516, doi: 10.1109/MASS.2014.85.

[20] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018, doi: 10.3390/e20100730.

[21] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015, doi: 10.1109/MCOM.2015.7120011.

[22] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 457–464, doi: 10.1109/DCOSS.2019.00091.

[23] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[24] M. Usman, M. A. Jan., X. He, and J. Chen, "P2DCA: A privacy-preserving-based data collection and analysis framework for IoMT applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1222–1230, Jun. 2019, doi: 10.1109/JSAC.2019.2904349.

[25] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[26] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: A two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019, doi: 10.1109/ACCESS.2019.2899721.

[27] A. Bengag, O. Moussaoui, and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," in *Proc. 3rd Int. Conf. Intell. Comput. Data Sci. (ICDS)*, Oct. 2019, pp. 1–5, doi: 10.1109/ICDS47004.2019.8942268.

[28] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational AutoEncoder and deep neural network," *Sensors*, vol. 19, no. 11, p. 2528, Jun. 2019, doi: 10.3390/s19112528.

[29] H. Zhang, X. Yu, P. Ren, C. Luo, and G. Min, "Deep adversarial learning in intrusion detection: A data augmentation enhanced framework," 2019, *arXiv:1901.07949*.

[30] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019, doi: 10.1109/ACCESS.2019.2903723.

[31] D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *Int. J. Inf. Manage.*, vol. 49, pp. 533–545, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.04.006.

[32] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Jun. 2019, doi: 10.1155/2019/7130868.

[33] J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101974, doi: 10.1016/j.adhoc.2019.101974.

[34] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Comput. Netw.*, vol. 148, pp. 164–175, Jan. 2019, doi: 10.1016/j.comnet.2018.11.010.

[35] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in networks," in *Proc. Cybersecur. Cyberforensics Conf. (CCC)*, May 2019, pp. 74–77, doi: 10.1109/CCC.2019.000-6.
[36] H. Nguyen, "IoT botnet detection approach based on PSI graph and DGCNN classifier," in *Proc. IEEE Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Sep. 2018, pp. 118–122.
[37] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A multimodal malware detection technique for Android IoT devices using various features," *IEEE Access*, vol. 7, pp. 64411–64430, 2019.
[38] J. Su, V. D. Vasconcellos, S. Prasad, S. Daniele, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf.*, vol. 1, Jul. 2018, pp. 664–669, doi: 10.1109/COMPSAC.2018.10315.
[39] S. M. P. Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad, and H. Homayoun, "Lightweight node-level malware detection and network-level malware confinement in IoT networks," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, pp. 776–781.
[40] J. J. Chiriyankandath, J. Jestine, A. Kamath, M. Khatib, and P. Nawal, "Automated data cleaning," Dept. Comput. Eng., Univ. Mumbai, Mumbai, India, Tech. Rep., Dec. 2021.
[41] D. Wagner, D. Heider, and G. Hattab, "Mushroom data creation, curation, and simulation to support classification tasks," *Sci. Rep.*, vol. 11, no. 1, Dec. 2021, Art. no. 8134, doi: 10.1038/s41598-021-87602-3.
[42] V. Shakya and R. R. S. Makwana, "Feature selection based intrusion detection system using the combination of DBSCAN, K-mean++ and SMO algorithms," in *Proc. Int. Conf. Trends Electron. Inform. (ICEI)*, May 2017, pp. 928–932, doi: 10.1109/ICOEI.2017.8300843.
[43] Y. K. Saheed and F. E. Hamza-Usman, "Feature selection with IG-R for improving performance of intrusion detection system," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 3, pp. 338–344, 2020.
[44] R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, "Active learning to detect DDoS attack using ranked features," *Comput. Commun.*, vol. 145, pp. 203–222, Sep. 2019, doi: 10.1016/j.comcom.2019.06.010.
[45] B. Chopard and M. Tomassini, "Particle swarm optimization," in *An Introduction to Metaheuristics for Optimization* (Natural Computing Series). Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-319-93073-2_6.
[46] S. O. Abdulsalam, S. Y. Kayode, H. M. Abiola, S.-I. T. Tosin, and A. N. Babatunde, "Student's performance analysis using decision tree algorithms," *Anale Seria Inform.*, vol. 15, no. 1, pp. 55–62, 2017.
[47] S. Sengupta, S. Basak, and R. A. Peters, II, "Particle swarm optimization: A survey of historical and recent developments with hybridization perspectives," *Mach. Learn. Knowl. Extraction*, vol. 1, no. 1, pp. 157–191, 2019, doi: 10.3390/make1010010.
[48] B. Chopard and M. Tomassini, *An Introduction to Metaheuristics for Optimization*. Cham, Switzerland: Springer, 2018, pp. 97–102, doi: 10.1007/978-3-319-93073-2.
[49] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in SDN-based networks," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, Jun. 2018, pp. 462–469, doi: 10.1109/NETSOFT.2018.8460090.
[50] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, Feb. 2016, pp. 1–5, doi: 10.1109/PlatCon.2016.7456805.
[51] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Proc. Comput. Sci.*, vol. 89, pp. 213–217, May 2016, doi: 10.1016/j.procs.2016.06.047.
[52] H. Zhang, S. Dai, Y. Li, and W. Zhang, "Real-time distributed-random-forest-based network intrusion detection system using Apache spark," in *Proc. IEEE 37th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Nov. 2018, pp. 1–7.
[53] Y. Y. Aung and M. M. Min, "An analysis of random forest algorithm based network intrusion detection system," in *Proc. 18th IEEE/ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. (SNPD)*, Jun. 2017, pp. 127–132, doi: 10.1109/SNPD.2017.8022711.
[54] B. Ingre, A. Yadav, and A. K. Soni, "Decision tree based intrusion detection system for NSL-KDD dataset," in *Proc. Int. Conf. Inf. Commun. Technol. Intell. Syst.*, vol. 84, Aug. 2017, pp. 207–218, doi: 10.1007/978-3-319-63645-0_23.
[55] Y. K. Saheed, T. O. Oladele, A. O. Akanni, and W. M. Ibrahim, "Student performance prediction based on data mining classification techniques," *Nigerian J. Technol.*, vol. 37, no. 4, p. 1087, Nov. 2018, doi: 10.4314/njt.v37i4.31.
[56] T. Nathiya and G. Suseendran, "An effective way of cloud intrusion detection system using decision tree, support vector machine and Naïve Bayes algorithm," *Int. J. Recent Technol. Eng.*, vol. 7, pp. 38–42, Jan. 2018.
[57] A. R. Syarif, "Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm," in *Proc. 11th Int. Conf. Inf. Commun. Technol. Syst.*, 2017, pp. 181–186.
[58] R. G. Jimoh, R. M. Yusuf, Y. O. Olatunde, and S. Y. Kayode, "Application of dimensionality reduction on classification of colon cancer using ICA and K-NN algorithm," *Anale Seria Inf.*, vol. 6, no. 10, pp. 55–59, 2018. [Online]. Available: http://anale-informatica.tibiscus.ro/download/lucrari/16-1-06-Olatunde.pdf
[59] F. Chen, Z. Ye, C. Wang, L. Yan, and R. Wang, "A feature selection approach for network intrusion detection based on tree-seed algorithm and K-nearest neighbor," in *Proc. IEEE 4th Int. Symp. Wireless Syst. Int. Conf. Intell. Data Acquisition Adv. Comput. Syst. (IDAACS-SWS)*, Sep. 2018, pp. 68–72, doi: 10.1109/IDAACS-SWS.2018.8525522.
[60] A. Singh, B. S. Prakash, and K. Chandrasekaran, "A comparison of linear discriminant analysis and ridge classifier on Twitter data," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, Apr. 2016, pp. 133–138, doi: 10.1109/CCAA.2016.7813704.

YAKUB KAYODE SAHEED (Member, IEEE) is currently an Assistant Professor with the American University of Nigeria. He has published in several local and international journals and conference proceedings. His research interests include intrusion detection, information security, bioinformatics, residue number systems, machine learning, and artificial intelligence. He is a member of the Internet Society, IAENG and SDWIC. He is also a Certified Network Security Specialist.

MICHEAL OLAOLU AROWOLO (Member, IEEE) received the bachelor's degree from Al-Hikmah University, Ilorin, Nigeria, the master's degree from Kwara State University, Malete Nigeria, and the Ph.D. degree from Landmark University, Omu-Aran Nigeria. He is currently a Faculty Member of the Department of Computer Science, Landmark University. He has published widely in local and international reputable journals. His research interests include machine learning, bioinformatics, datamining, cyber security, and computer arithmetic. He is a member of IAENG, APISE, SDIWC, and an Oracle Certified Expert.