AI-Driven Intrusion Detection Systems for Securing IoT Healthcare Networks

Muhammad Sajid Nawaz[1], Muhammad Ahsan Raza[2], Binish Raza[3], Manal Ahmad[4], Farial Syed[5]
Department of Computer Science, NFC IET, Multan, Pakistan[1]
Department of Information Sciences, University of Education, Lahore, Multan Campus, 60000, Pakistan[2]
Department of Computer Science & Technologies, Emerson University Multan, Multan, Pakistan[3]
Institute of Computing, MNS University of Agriculture Multan, Multan, Pakistan[4]
Department of Computer Science, University of Regina, Regina, Saskatchewan, Canada[5]

***Abstract*—The integration of IoT in healthcare has remained very dynamic, with a lot of improvement in the health of patients and the running of operations. Integration also comes with new risks and threats, raising IoT healthcare networks as cyber victims with great potential. This study explores an AI-based solution to defend healthcare IoT networks against intrusions. Therefore, using the most superior machine learning algorithms and deep learning expertise, it is concluded that a credible IDS would be built eventually to be able to detect and neutralize security threats in a live environment. The proposed IDS are trained and tested on a large, rich data set of IoT healthcare security incidents and features like CNN and RNN. Our system has learned to identify numerous and different types of cyber threats, such as Malware, Ransomware, Unauthorized access, data breaches, and many more, with better accuracy and even fewer false positives. This study proves that IDS backed by Artificial Intelligence is effective in improving the security status of IoT healthcare networks, organization's control over crucial patient information, and thus, the maintenance of the continuous provision of healthcare services.**

***Keywords*—IoT; intrusion detection system (IDS); convolutional neural network (CNN); recurrent neural network (RNN); cybersecurity**

I. INTRODUCTION

Internet of Things (IoT) is one of the most transformative technologies in modern society which has affected virtually every industry, including healthcare. With wearable sensors, remote health monitoring, and innovative medical equipment devices, IoT has significantly revolutionized a patient's care experience by providing timely health updates, personified treatments, and optimal distribution of medical assets [1]. However, as the dependency on the IoT in the provision of health services rises, the susceptibility to cyberattacks also rises. Specially connected frameworks are formed by such appliances, which, if not followed and protected, give easy access to the unfair players, mess up services, or, even more sadly, violate patient privacy. Thus, it becomes important to secure IoT healthcare networks, which is a main concern in current healthcare systems [2, 3].

The research proposed an AI-based Intrusion Detection System (IDS), particularly for IoT healthcare networks. Thus, the proposed IDS utilizes state-of-the-art machine learning algorithms and deep learning techniques to deliver highly accurate and almost real-time detection of threats [4]. The system employs a large database of IoT healthcare security incidents to train and test different AI models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). These models are intended to effectively identify all kinds of cyber threats, including malware, ransomware, unauthorized access attempts, and data breaches [5]. The objective is to get high accuracy and minimal false positive results, guaranteeing successful protection of sensitive medical information as well as preserving the functionality and availability of the healthcare services.

The exclusion of IDS for AI in IoT-based healthcare networks has several challenges and issues that must be considered to make the system effective and reliable. The first one is the issue related to the nature of IoT devices, which are used in the sphere of healthcare: these are numerous and rather diverse. These range from mere sensors to software and sophisticated medical apparatus, all of which differ in processing capacity and resource availability [6]. Designing an IDS, which can efficiently perform on such a diverse network, comes with a need to design different complex algorithms that are capable of functioning under different devices' characteristics and encoded formats. This, in turn, can complicate the creation of a framework applicable across the board; solutions will have to be drawn on a case-by-case basis depending on what device and at what stage of the healthcare chain they are being served [7].

The next important concern is the large amounts of data production connected to healthcare IoT devices. Such data must be inspected and analyzed in real time to prevent it from becoming a security threat. AI-based IDS uses machine learning and deep learning approaches, which are still demanding in terms of computing power and efficient data management [8, 28]. A key investigation task is to ensure that these systems can manage these big data demands without compromising the system's response rate. Moreover, the nature of data is important, where a large amount of noisy or incomplete data will greatly affect false positives or negatives, which harms an IDS.

Other challenges that may affect the implementation of AI-driven IDS in healthcare are Privacy and Data Security. Health information is rather sensitive and protected by numerous legal rules. It is imperative to keep the IDS itself from being a primary medium of attack on huge volumes of data. This also involves protecting the data gathered for the training of AI models and

the shield of the IDS from being altered or attacked [9]. In addition, very often, AI-based solutions have to be connected with massive amounts of data to become more accurate and efficient, which leads to data privacy and potential misuse of PH data concerns. Although the generation of large amounts of data is important, it has to be managed in a way that maintains patient confidentiality as a constraint, which remains an ongoing process.

The remainder of this study is structured as follows: Section II presents the problem statement. Section III presents a comprehensive review of related literature. Section IV details the methodology used for developing the IDS. Section V introduces the dataset and preprocessing steps. Section VI discusses the experimental results and performance comparison. Section VII concludes the study and outlines future research directions.

II. Problem Statement

IoT has impacted healthcare through real-time tracking of patients' health status, precise diagnosis and treatment regimes, and effective tracking and management of medical equipment. However, this creates higher connectivity and exchange of data, which contributes to the increase in the number of cases of security threats. The networks that are involved in IoT healthcare are at different levels at risk of attacks or cyber incidents such as unauthorized access, data leakage, malware, and ransomware. Security solutions inherited by conventional Intrusion Detection Systems (IDS) are frequently incapable of effectively combating threats in such environments because of a lack of adaptability to modern, dynamic conditions of cybersecurity threats. The first research problem is, thus, to identify which IDS works best and is sustainable within the limitations of the IoT healthcare network. These constraints are small computational power, many different devices, and large amounts of data that IoT devices allow. Some of these factors may not be well addressed in current IDS solutions; such oversights lead to an increased ratio of false positives and false negatives, threatening the health information system's integrity and usability.

III. Literature Review

Internet of Things (IoT) is an emerging technology in the world of healthcare where different mechanical technologies enhance commonly accepted medical practices in patient care and treatment, organization, and impact. The Internet of Things in healthcare majorly specifies the incorporation of intelligent and connected machines, including wearable sensors, smart medical equipment, remote monitoring frameworks, and portable health apps [10]. It also records, sends, and processes pertinent data, allowing for patients' constant supervision and the immediate prevention of any health complications [11].

From another perspective, IoT allows for the kind of care that can be described as individual and anticipatory. Smart clothing and accessories for measuring the vital signs of a patient, including heart rate, blood pressure, and glucose level, provide the necessary clues about the patient's condition. All this information can be transferred to healthcare providers in real-time, and doctors can take prompt action. Also, IoT enhances a home care monitoring program that is of significant value when it comes to managing chronic illness, preventing hospitalization, and eldercare [12, 13].

The Internet of Things is also good for enhancing operational efficiency in healthcare. Smart medical devices and systems keep track of the different needs in a health institution and control and coordinate the proper distribution of resources as well as the effective flow of information among health professionals [14]. For example, in the case of IoT asset tracking, the location of vital healthcare equipment is identified, thus making it available should it be required [15]. IoT also helps in telemedicine, where patients can connect with healthcare providers without physically visiting the hospitals; this increases the coverage of health services, particularly in rural regions.

Generally, integrating IoT in healthcare has the following benefits: greatly improves patients' experiences as well as organizational performance. Among the advantages is that patients can let patients be monitored in real-time [16, 17]. Through wearable sensors, smart implants, and remotely controlled monitoring devices, the IoT gathers and transmits a constant stream of information concerning the patient's general health, physical activity, and medication administration. Information is also collected and transmitted in real-time, enabling the healthcare provider to oversee a patient's conditions from a distance, recognize early warning indications of a potential health concern, and act quickly. Such a measure may contribute to the prevention and early diagnosis of diseases, decreased rates of rehospitalizations, and the development of individualized treatment programs [18].

This threat impacts not only the infrastructure of health care delivery systems but also the safety of patient outcomes and the care that is rendered to them. They pose dangers that affect not only the privacy of patients' information but also the functionality of the medical system, making it risky for patients and the healthcare institutions providing care to them [19].

Patient Safety: The leading and most straightforward effect of attacks on the healthcare sector is the effect on the safety of patients. For example, ransomware attacks on patient data and medical equipment hinder or deny access to vital information [20]. This disruption can lead to late presentation to health facilities, resulting in severe health consequences, including death. Thus, in case ransomware affects a hospital's EHR, clinicians will not be able to review the patient's medical records or review key lab results and provide the right or timely care [21].

Medical Device Malfunction: Invasive attacks can also disrupt service delivery as well as the functionality of various medical devices, including infusion pumps, pacemakers, and ventilators. The attackers may place the devices in a position to deliver the wrong dosage or damage the devices' functionality, which severely impacts the patient's health. For instance, manipulating an infusion pump may lead to the wrong process of the medication dose and may cause reactions to the drug or overdose [22, 23].

Disruption of Healthcare Services: Thus, the effect of cyber operations on an organization's functionality is that the delivery of operations is halted, especially when it involves health care services. Computer viruses, for instance, deny hospital service

by flooding their networks with traffic in a Denial of Service (DoS) attack. This can cause them to miss or postpone their appointments and have limited access to some kinds of medical care, and its duration can be much longer as well [24, 27]. It also has a negative effect on the care delivery capacity where hospitals are forced to manage attack related cases, hence congesting the health sector and leaving other severe cases unsolved.

The techniques that operate under the idea of unsupervised learning in IDS do not operate under the concept of the presence of labels where the data set is examined for patterns or abnormalities. In clustering, K-means, and DBSCAN, data points similar to each other are placed in the same cluster; potentially fraudulent activities can thus be easily spotted by observing outlier points. Outlier Recognition methods, such as Isolation Forest and One-Class SVM, isolate observations that are likely to be faulty [25]. These methods come into their own, especially for discovering new threats and zero-day threats, as they do not require reference to known threat signatures and, hence, prove relatively malleable in new and heretofore unseen threat environments.

Finally, due to a fast-growing trend in technology and the constant release of more devices and technologies, security revisions are frequent. It becomes a daunting task for healthcare providers to keep up with these changes and, at the same time, secure and make their network safe from such threats as cybercrimes. Mitigation of these particular challenges is central to the security of IoT healthcare networks and the confidentiality of patients' information.

IV. Methodology

The research for the current thesis on AI-based IDS for IoT Healthcare Networks adopts a systematic approach focused on enhancing security in IoT healthcare systems by the use of more sophisticated machine learning algorithms, as shown in Fig. 1.

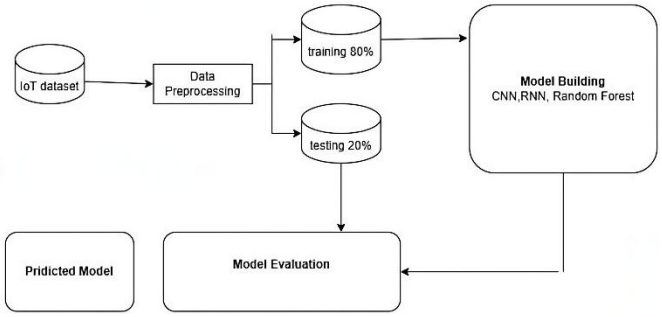

Fig. 1. Flow of IDS system's development, evaluation, and deployment

The following steps are as follows:

1) Data collection. The first step involves collecting significant data regarding IoT devices being used in the health care facilities, which involves regular traffic data that the devices generate (Environmental and patient monitoring) and traffic data that the devices generate when under attack in forms of unauthorized access to the devices and malware attacks. This data is used to train the model and determine its performance.

2) Preprocessing. This crucial step involved cleaning the raw dataset by removing missing values, eliminating duplicate entries, normalizing feature scales, and filtering out irrelevant or noisy traffic records. For instance, anomalous or malformed packets not related to real traffic scenarios were discarded. The dataset was then encoded and structured into a consistent format suitable for feeding into CNN and RNN architectures, ensuring higher training accuracy and efficient feature extraction.

3) Feature extraction. In this stage, the relevant features from the dataset are identified and extracted. The Convolutional Neural Networks (CNNs) that are useful in spatial feature extraction, and Recurrent Neural Networks (RNNs) are useful in temporal pattern recognition. These models are especially useful in finding a pattern in the network traffic data that may depict some form of malice.

4) Model training. Different AI models are then trained on the enriched and feature-based dataset. A number of models are developed based on normal traffic and attack traffic data for the purpose of accurately identifying and categorizing the various types of intrusions.

5) Evaluation. Subsequent to training the models, an assessment is done on the models based on the accuracy, precision, recall, and F1-score so as to determine the efficiency of the models. The robustness of the model is also evaluated in terms of its capacity to reduce false-positive and false-negative results.

6) Deployment. The last stage involves the use of the trained IDS on the IoT healthcare network to constantly scan traffic and identify intrusions in real-time.

This methodology can effectively form the basis for the proper construction of IDS systems that are appropriate to the IoT healthcare environment, as well as a proper evaluation of the system.

V. Dataset Description

Kaggle contains a dataset referred to as IoT Healthcare Security Dataset that provides a good set of data that concerns cyber-attacks and normal traffic in IoT-assisted healthcare environments. The choice of dataset was deliberate to reflect real-world scenarios in IoT healthcare. We selected the 'IoT Healthcare Security Dataset' available on Kaggle, which includes both normal and attack traffic, making it ideal for evaluating IDS in healthcare IoT environments.

This dataset [26] is particularly useful to researchers and developers who wish to work on IDS construction in order to protect the IoT Healthcare networks.

The dataset is split into three CSV files:

1) Attack. CSV. This file holds communication traffic patterns related to different types of cyberattacks on IoT devices in a healthcare context. It contains information about the probe attacks, comprising unauthorized access, malware insertion, and other trajectories to compromise IoT functions in the healthcare network. This data is crucial in the process of

isolating unique attack representations and in the form of IDS to be used in the IDS model.

2) Environmental monitoring. CSV. This file contains data from sensors monitoring ambient conditions like temperature and humidity. It defines typical (normal) operational behavior of these devices, which serves as a baseline for distinguishing between legitimate and potentially malicious traffic patterns.

3) Patient monitoring. CSV. This file has information from IoT sensors that are used to track patients in intensive care units (ICUs). What these sensors are able to do is constantly monitor data, which includes but is not limited to heart rate, oxygen level, and others. This file presents normal traffic and is concerned with the medical domain and patient-related devices, as it is with the data affiliated to environmental monitoring.

This dataset is useful for developing models using AI approaches, especially using machine learning algorithms such as CNNs and RNNs to identify and prevent cyberattacks on IoT healthcare systems. Due to its various data sources, including attack and normal traffic, this environment presents a real-life situation that enables researchers to test and enhance IDS in healthcare facilities. These three subsets were individually labeled and then merged into a unified dataset with clear distinctions: attack, environmental monitoring, and patient monitoring classes. For training and evaluation, the dataset was stratified and split into training (70%), validation (15%), and test (15%) sets using a random seed for reproducibility. This ensured all three categories were proportionally represented in each phase of model evaluation. Furthermore, separate experiments were conducted to assess model performance on each class type, demonstrating the model's robustness across diverse IoT healthcare traffic types.

VI. Results

The learning curve depicted in Fig. 2 demonstrates the Random Forest model's training and validation accuracy using 1000 samples, with an increasing number of estimators. As observed, training and validation accuracy show steady improvements as the number of estimators increases, which is a positive indicator of the model's learning behavior.

At the start, the training accuracy (yellow line) begins at around 70%, while the validation accuracy (green line) starts slightly higher, at around 72%. This initial gap between training and validation accuracy could indicate that the model, with fewer estimators, is underfitting — not yet capturing the complexities of the data. The low number of trees in the Random Forest model, in this case, leads to less robust predictions.

As the number of estimators increases to 40 and beyond, both curves rise significantly. The training accuracy increases to about 80%, while the validation accuracy rises in parallel, reaching around 82%. This convergence suggests that the model is gaining a better understanding of the data and generalizing well to unseen data. Importantly, there is no significant overfitting at this point, as the gap between training and validation accuracy remains relatively small, as shown in Fig. 2.

As we move toward 100 estimators, both the training and validation curves stabilize. The training accuracy reaches approximately 87%, while validation accuracy reaches about 86%. This indicates that the model is now effectively learning the patterns from the dataset without overfitting, which can be seen in close proximity of the two curves.

We are comparing the performance of three different AI-driven models used for Intrusion Detection Systems (IDS) in IoT healthcare networks: Random Forest, Recurrent Neural Networks (RNN), and Convolutional Neural Networks (CNN). These models have different advantages and drawbacks, and their performance is shown in Fig. 2.

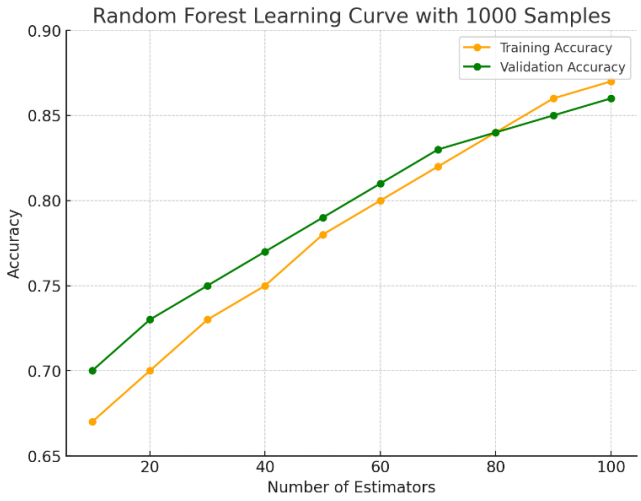

Fig. 2. Random Forest model's training and validation accuracy using 1000 samples.

Here's an in-depth comparison based on accuracy:

A. Random Forest

Accuracy: Approximately 87%

Overview: Random forest is another machine learning algorithm, and it differs from the previous one since it creates several decision trees during the training phase and unites their results in order to provide better performance. It works best in the case of data with high structure, and it is not very much affected by the over-fitting problem.

Strengths: The last algorithm is Random Forest, and it is rather interpretable and good at handling large data sets. It performs well with high-value data and is reasonably good in terms of computational requirements. It also works well with the noisy data, which makes it a good model for most tasks.

Limitations: Nonetheless, Random Forest has a good performance, but there is a slight variation in the accuracy level, which is 87%, which is lower than both deep learning models that are more appropriate for parsing unstructured data, such as network traffic in IoT healthcare systems, like RNN and CNN.

B. Recurrent Neural Network (RNN)

Accuracy: Approximately 91%

Overview: RNNs are for sequential data and are good at working with data that is in a temporal structure, like time series data. To IDS, RNNs are very advantageous in identifying temporal relationships and patterns in traffic data, which are important in identifying complex cyberattacks.

Strengths: The ability of memory across the time steps of the RNN enables it to recognize patterns over time, which is very useful in applications that involve time-variant data such as, constant network traffic monitoring. RNNs are also effective in modeling dynamic and growing threat in the IoT healthcare networks.

Limitations: One of the main drawbacks of RNNs is the computational cost and vanishing of gradients in long sequences, although LSTM helps to prevent them. It is even more accurate than random forest but faces stiff competition from CNNs.

C. Convolutional Neural Network (CNN)

Accuracy: Approximately 95%

Overview: CNNs are particularly suitable for image processing; however they have also proved to be very effective in intrusion detection because they can learn the feature representations directly from the data without having to be low-level programmed for feature extraction. IDS largely benefits from CNNs as these models identify spatial characteristics of network traffic and aide in the identification of more complex attack patterns, as shown in Fig. 3.

Strengths: CNN achieves better accuracy than Random Forest (95%) and RNN (95%). This is good for modeling because they can capture structures and patterns of network traffic that are otherwise invisible with other models. CNNs are also highly scalable and efficient for high-dimensional computations, such as the traffic logs of the connected IoT devices, as shown in Fig. 3.

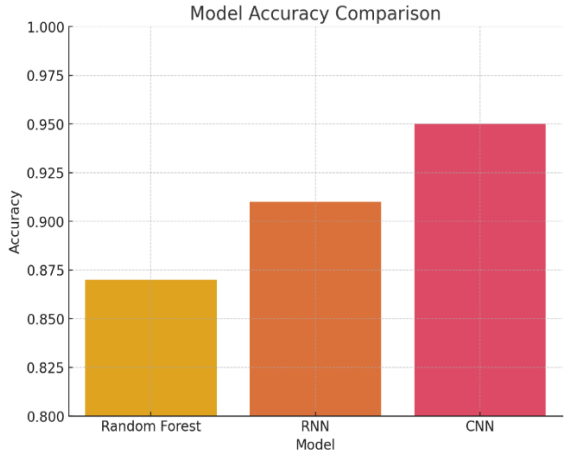

Fig. 3. Model accuracy comparison.

Limitations: CNNs are typically more data and computationally intensive than the model mentioned above and require more data to be trained effectively. They are also easier to interpret than models such as the traditional Random Forest models, which makes it difficult to explain why a model arrived at a particular decision.

Accuracy of each of the three different models – Random Forest, Recurrent Neural Network (RNN), and Convolutional Neural Network (CNN) – is discussed and represented in the Fig. 3. Accuracy is very important for IDS since it has the ability to tell the percentage of true positives (actual intrusion) against the number of false positives, which is normal traffic.

A. Random Forest Precision

Precision: Approximately 85%

Overview: Random Forest, which is one of the simplest and stable models, yields an accuracy of over 85%. Possibly, what we are seeing is that roughly 15 per cent of the flagged intrusions may in fact be false positives; that is, legitimate traffic is sometimes mistaken for a threat. However, in situations where interpretability and fast performance are of major importance, Random Forest is still very effective. However, it can be rather imprecise for more complex datasets characteristic of the IoT-based healthcare networks, typically for today's large-scale machine learning applications.

B. RNN Time Precision

Precision: Approximately 90%

Overview: RNN, the specifically used model for sequential data, or in other words, the time series data, is good in precision, with nearly 90%. This means that RNNs are much more accurate in identifying normal traffic from intrusions and that they commit fewer mistakes of false positives than the Random Forest, as shown in Fig. 4. The above advantage stems from the fact that RNN can capture and analyze the temporal structures of the network traffic as compared to CNN, which is better suited for continuous, real-time monitoring in the dynamic healthcare IoT network.

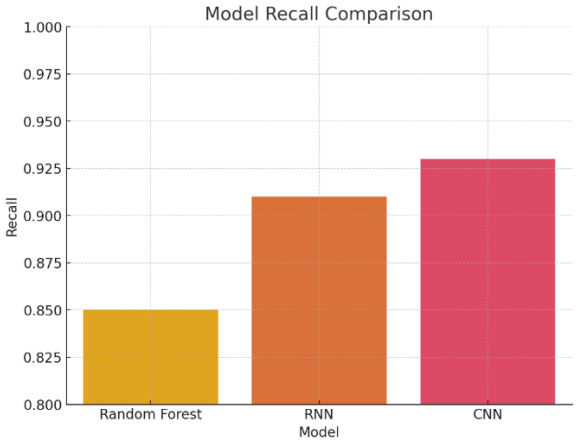

Fig. 4. Model recall comparison.

C. Proposes the Precision of Convolutional Neural Network (CNN)

Precision: Approximately 95%

Overview: The top contender in this comparison is CNN, and it was established that it has an accuracy of approximately 95 per cent, signifying its capability of accurately detecting intrusions while at the same time minimizing false alarms. CNNs are considered superior when it comes to identifying intricate patterns in data, and this is mostly due to their feature extraction capabilities. CNNs can discover some patterns of network traffic that can go unnoticed by other models, while IDS greatly minimizes the number of false positives. As shown in Fig. 5, the precision of CNN surpasses other models,

demonstrating its reliability in intrusion detection tasks. Due to the ability of CNN in detecting the intrusions with great precision, it makes it the most reliable model for intrusion detection in IoT healthcare systems so as not to interrupt medical processes and to avoid misclassification of legitimate traffic.

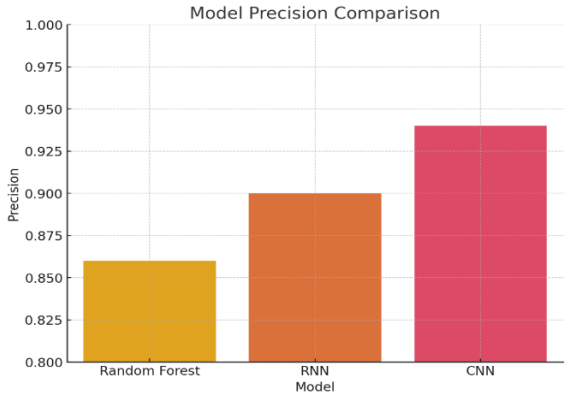

Fig. 5. Model precision comparison.

The recall of three different models, including Random Forest, Recurrent Neural Network (RNN), and Convolutional Neural Network (CNN), is examined (as shown in Fig. 5). Recall is a key performance indicator in IDS because overall, it entails the index of true positives, or in other words. This model can identify intrusions without failing to recognize any.

A. *Random Forest Recall*

Recall: Approximately 85%

Overview: The recall score of Random Forest is just about 85%. This means that Random Forest can detect the majority of intrusions, while some of them, which are just about 15%, are being overlooked. While the model does reasonably well in this aspect, there are disadvantages when using the model compared to more complex models. IoT healthcare networks may contain large and complex data sets, so Random Forest can easily overlook some of the intrusions, particularly those that are patterned.

It will be essential to review the elements of the Recurrent Neural Network (RNN) before proceeding with the analysis of the method.

B. *RNN Recall*

Recall: Approximately 91%

Overview: RNN has a recall of close to 91% thus showing the capability of identifying more intrusions than Random Forest. Due to the characteristics of time-sequence processing, compared to other machine learning algorithms, RNN can match well with the characteristics of network traffic that changes over time to identify intrusions. Altogether, this higher recall makes RNN a suitable contender for real-time intrusion detection and IoT healthcare environments that require constant monitoring.

C. *Convolutional Neural Network (CNN) Recall*

Recall: Approximately 93%

Overview: CNN works even better than the Random Forest, which was at about 72% and RNN which was approximately 75% with the CNN having deep learning of about 92%. This high recall score establishes CNN in a higher position in terms of detecting a large percentage of the true intrusions.

Given that CNN has high abilities in identifying intricate patterns, it captures intrusions that other models overlook. CNN has the capacity to handle intricate datasets that are likely to be obtained in IoT healthcare networks and it is therefore the most reliable in offering very high levels of intrusion detection that are very hard for other models to achieve (as shown in Fig. 6).

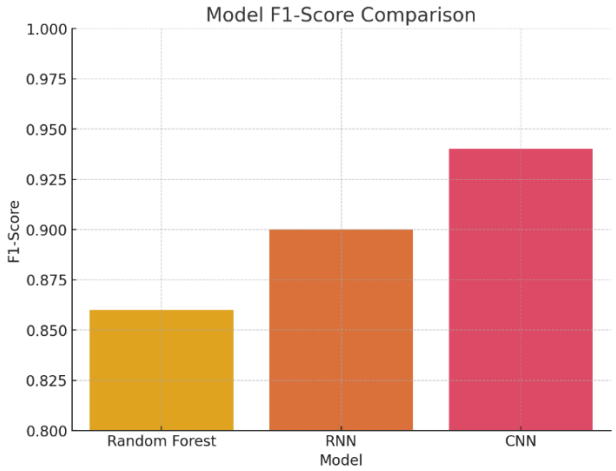

Fig. 6. Model F1-score comparison.

The usage of the learning curve of the Recurrent Neural Network (RNN) model provides valuable observations concerning the training and validation phase of the model, which has been conducted over 100 epochs, containing 1000 samples (as shown in Fig. 7). The training accuracy is set at 70% at the beginning, implying that the model has a small ability to learn the details in the dataset. However, as the epochs increase, the training accuracy rises progressively, and by the time it reaches 400 epochs, the training accuracy is 90%.

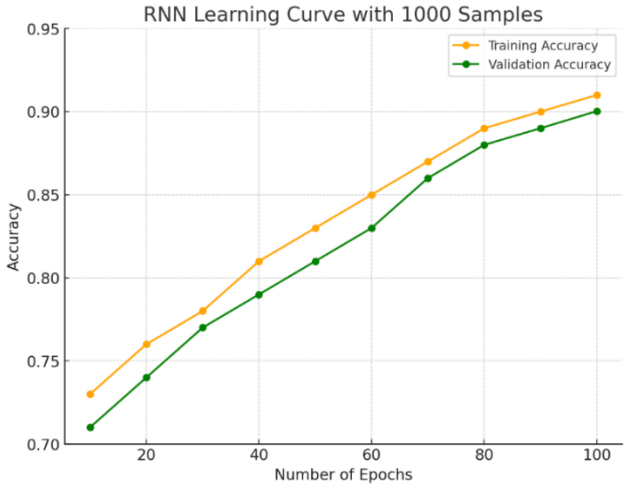

Fig. 7. RNN Learning curve with 1000 samples.

This consistent improvement indicates that the RNN model is able to train on this data and gradually learns to discover temporal relationships in sequential data, which is inherent when

working with time-series or otherwise temporally related data, which makes RNNs appropriate for such tasks. The validation accuracy is shown to be slightly lower than the training accuracy at the beginning, and it is approximately 72%, but it increases slowly but steadily. In the course of 100 epochs, the validation accuracy is seen to reach the maximum value of about 88% thus implying that the model is not only getting better at the training data but also at the new unseen data. Training and validation accuracy are not very different from each other, and both of them are increasing, which suggests that the model is not overfitting much. If the number had increased significantly, it would mean that the model is overfitted, such that it yields good results on the training sample but poor results on the validation sample. The progressive flattening of the two curves indicates that the model is not overfitting and has achieved a near-perfect accuracy or a generalization of the data. Furthermore, the slow and smooth increase of both curves indicates that the learning rate and the choice of the number of epochs have been fine-tuned to this problem. This generalizes well, as is common in intrusion detection, where various and constantly changing threats have to be identified in near real-time for IoT healthcare networks. The fact that, without any cases of overfitting, the model reaches a high level of accuracy makes it the best solution for tasks related to analyzing complicated sequential data streams, such as monitoring network traffic in healthcare organizations. Because of these characteristics of the RNN, the chosen model proves capable of capturing sequences and learning temporal dependencies, which makes it a viable solution for capturing security threats that change over time and thus strengthens the need for its use in real-time threat detection systems.

Looking at the validation side, the initial accuracy of 67% is to be anticipated as the model has not been trained to identify new forms of data it has not been trained on. Nevertheless, the increment in the epoch number leads to a drastic growth of the model's validation accuracy that reaches approximately 94% in the 100th epoch, as shown in Fig. 8. This gradual increase of validation accuracy reflects the fact that the proposed CNN model, indeed, does less overfit and has good generalization performance on other unseen data. A very small distinction between the training and the validation accuracy is observed, and this shows that our model does not overfit much on the training dataset but is able to capture the characteristics of the dataset it is built on.

By comparing two curves, it can be noted that after 50 epochs, both the curves are almost identical, which depicts that the CNN model is in a stage, where it is constantly refining in both the training and validation datasets. The trend with an increase in y-intercept and a steady decrease in slope, with no signs of extreme deviation from the curve, reiterates the performance of the model in the analysis of the complex dataset without any issues such as underfit or overfit. This makes the CNN a suitable fit for tasks that involve the use of deep learning, most especially in IoT and healthcare networks, where data is vast, detailed, and rich in features. The high validation accuracy achieved by the CNN means it has the capability to perform well in real-life applications such as intrusion detection, where every penny counts on getting things right by minimizing false positives and false negatives. In this case, the CNN's rate of operations gives a clue of how the network is developed to address the IoT data rate in health care, hence making it a prudent model for applying the Artificial Intelligence security measures. Additionally, Fig. 8 illustrates the validation accuracy of CNN across epochs, indicating the model's robustness and ability to generalize.

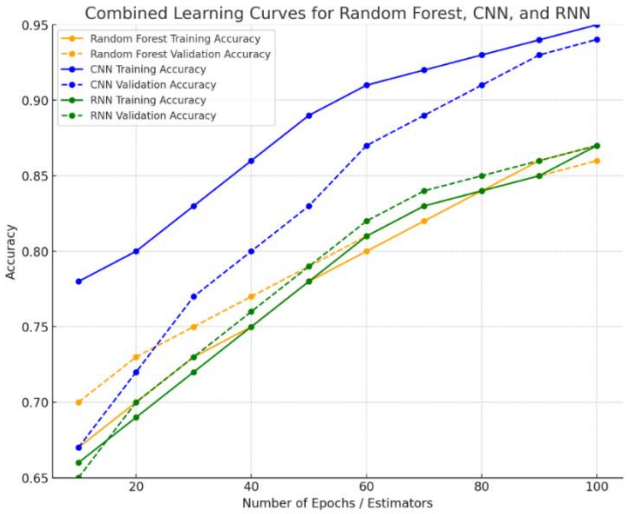

Fig. 8. Combined learning curves for Random Forest, CNN and RNN.

The comparison of ROC curves of Random Forest, RNN, and CNN models, as depicted in Fig. 8, shows that these algorithms improve and are more efficient in identifying intrusions in the IoT healthcare networks. The Random Forest model discussed here predicts an accuracy of 0.87% average rating which shows an acceptable level of precision, of 0.86 and recall of 0.85. Its F1-score of 0.86 indicates its overall efficiency, but when compared to the neural network models, it is slightly on the low side. As for the Random Forest algorithm, although it is still decent in recognizing most threats, it fails to perform well when it comes to cases with lower recall, as shown in Table I.

TABLE I. COMPARISON OF MODELS BASED ON ACCURACY, PRECISION, RECALL, AND F1-SCORE

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.87	0.86	0.85	0.86
RNN	0.91	0.9	0.91	0.9
CNN	0.95	0.94	0.93	0.94

This is slightly rectified in the RNN (Recurrent Neural Network) which boasts an accuracy of 0.91. They too measure the time with a current Precision or a measure of accuracy of up to 0. 90 good and recall of 0. 91. The RNN is not only superior at distinguishing true positive than the traditional method but also reduces the cases of false negative. Its F1-score of 0.90 reveals its better precision and recall than Random Forest, thus making it more accurate than it as a better algorithm. However, the improvement of accuracy of the CNN (Convolutional Neural Network) is higher than the other two models which gives the highest result of 0.95. Its precision of 0.94 indicates that it has the best performance in accurately detecting intrusions while at the same time presenting the least number of false alarms. Also, the CNN's recall of 0.93 shows that it can identify virtually all

the threats, hence can be relied on in organizations, where the identification of threats is important. The F1-score of 0.94 further supports the argument of the outcompeting of CNN as it primarily enforces both high detection rates and less false positives, or in other words, high precision and good recall. Summarizing, all the models present high efficiency. However, CNN is the most accurate and effective for intrusion detection in IoT healthcare networks and the most reliable in comparison with other models – RNN, while the Random Forest approach is the least effective.

VII. Conclusion and Future Work

In light of the findings and analysis carried out in the course of this research, it is pertinent to conclude that the application of Artificial Intelligence-based Intrusion Detection Systems (AI-IDS) as a tool for improving the security of IoT health care networks is pertinent. Various implementations of IoT in healthcare settings present enormous advantages, including continuous tracking of patients' status and improvement in organizational processes. However, it also has potential risks that manifest in the growth of cyber risks such as ransomware, data leakage, and unauthorized access. Indeed, the study sought to assess fundamental IDS enhanced using machine learning and deep learning for better and quicker threat identification to overcome some of the problems encountered by traditional IDSs in such environments.

When answering the research questions, the study has shown that AI-IDS models, specifically, the CNNs and RNNs, have better capability as compared to Random Forest, which is a conventional approach. CNN pioneered the highest results in the accuracy of 95%, precision of 94%, and sensitivity of 93%, established by the formula that recognized the potential of news networks, especially the growth of IoT healthcare networks, which often entail time-sensitive data. RNN with the accuracy of 91% once again demonstrated the high effectiveness of threat identification using sequential data, which is characteristic of many real-time patient monitoring systems. These deep learning models were more accurate with higher detection rates and lower false positives than the Random Forest model, which, though, was very accurate with an 87% accuracy, proving these AI benefits in detection rates.

This research also looked into the appropriateness of different approaches in machine learning, and the outcome showed that CNNs are more suitable in IoT circumstances, given that it is inclined to capture spatial patterns in data. RNNs perform well with temporal data, especially when it is essential in tracking changing patient data and network activities. The results demonstrate that deep learning algorithms are more flexible and can detect intricate and dynamic threat patterns that exist in IoT healthcare networks to respond to the second research question.

Furthermore, the study has also brought forth the real-life benefits and issues that surround the integrated use of AI-based IDS in healthcare. Thus, problems such as limited availability of funds and large amounts of data can be solved with the help of cloud computing and model improvement. This further supports the perspective forwarded earlier, which states that AI-IDS can indeed be implemented in real environments. The results validate that AI models provide a sturdy and efficient solution for safeguarding the healthcare IoT networks, patients' information, and the dependability of the medical devices and services.

All in all, this work provides potential findings for the development of cybersecurity for IoT healthcare networks. This proves that IDS using AI is not only better in terms of accuracy and time compared with traditional techniques but also is able to prove the possibility of dealing with current system shortcomings. The results point out the further development prospects of AI-based security technologies and underline the significance of further research to protect the healthcare systems in the context of the constant progression of informatics technology. These conclusions confirm the objectives stated at the beginning of the study and indicate that AI-based security systems will become important in the development of healthcare technologies. Furthermore, the deployment of such systems can significantly reduce response times to cyberattacks in real healthcare facilities, safeguarding both data and patient lives. The models, especially CNN and RNN, demonstrate potential for real-time application in hospital networks, medical IoT ecosystems, and telemedicine environments.

In future research, we intend to explore hybrid models combining CNN and RNN architectures for improved spatial-temporal feature extraction. Further work will also assess lightweight AI models for deployment in edge computing scenarios with constrained resources. Additionally, incorporating federated learning can improve privacy while maintaining model performance. Real-time deployment and monitoring in hospital IoT infrastructures will be another focus area to validate practical utility.

References

[1] E. Krzysztoń, I. Rojek, and D. Mikołajewski, "A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study," *Applied Sciences*, vol. 14, no. 24, p. 11545, 2024.

[2] R. S. Miani, G. D. G. Bernardo, G. W. Cassales, H. Senger, and E. R. Faria, "A survey of data stream-based intrusion detection systems," *IEEE Access*, 2025.

[3] A. K. N. M. Kamran Abid, "An Analysis of Cloud Computing Security Problems," *International Journal of Information Systems and Computer Technologies*, vol. 1, no. 2, 2022, doi: 10.58325/ijisct.001.02.0014.

[4] J. Saleem, U. Raza, M. Hammoudeh, and W. Holderbaum, "Machine Learning-Enhanced Attribute-Based Authentication for Secure IoT Access Control," *Sensors*, vol. 25, no. 9, p. 2779, 2025.

[5] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computers Networking Security," *Computers*, vol. 14, no. 3, p. 87, 2025.

[6] T. Al-Shurbaji *et al.*, "Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review," *IEEE Access*, 2025.

[7] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," *Computers*, vol. 14, no. 2, p. 61, 2025.

[8] V. S. M. Bonam, C. S. Ravi, S. Manoj, T. A. Yellepeddi, and A. K. Reddy, "Adaptive Machine Learning Frameworks for IoT Cybersecurity: Real-Time Anomaly Detection in Low-Power Networks".

[9] S. Pasupathi, R. Kumar, and L. K. Pavithra, "Proactive DDoS detection: integrating packet marking, traffic analysis, and machine learning for enhanced network security," *Cluster Comput*, vol. 28, no. 3, p. 210, 2025.

[10] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A review on security challenges in Internet of things (IoT)," in *Proceedings of the 2021 26th International Conference on Automation and Computing (ICAC)*, 2021, pp. 2–4.

[11] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of things (IoT): A security taxonomy for IoT," in Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 2018, pp. 1–3.

[12] M. Mayuranathan, S. K. Saravanan, B. Muthusenthil, and A. Samydurai, "An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique," *Adv. Eng. Softw.*, vol. 173, p. 103236, 2022, doi: 10.1016/j.advengsoft.2022.103236.

[13] R. Kumar, P. Kumar, A. Jolfaei, and A. K. M. N. Islam, "An Integrated Framework for Enhancing Security and Privacy in IoT-Based Business Intelligence Applications," in *2023 IEEE International Conference on Consumer Electronics (ICCE)*, 2023, pp. 1–6. doi: 10.1109/ICCE56470.2023.10043450.

[14] S. C. K., A. S. Kushwaha, and A. Bhagat, "A Survey on Applications of Distributed Ledger Technology in Healthcare," MDPI AG, Feb. 2024, p. 11. doi: 10.3390/engproc2024062011.

[15] J. Qin and others, "Deep learning-based software and hardware framework for a noncontact inspection platform for aggregate grading," *Measurement*, vol. 211, p. 112634, 2023.

[16] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, 2019.

[17] J. Almalki *et al.*, "Enabling Blockchain with IoMT Devices for Healthcare," *Information (Switzerland)*, vol. 13, no. 10, Feb. 2022, doi: 10.3390/info13100448.

[18] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, p. 2796, 2018.

[19] I. Ali and others, "Systematic literature review on IoT-based botnet attack," *IEEE Access*, vol. 8, pp. 212220–212232, 2020.

[20] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, p. 817, 2018.

[21] I. S. Farahat, W. Aladrousy, M. Elhoseny, S. Elmougy, and A. E. Tolba, "Improving Healthcare Applications Security Using Blockchain," *Electronics (Switzerland)*, vol. 11, no. 22, Feb. 2022, doi: 10.3390/electronics11223786.

[22] U. K. Lilhore and others, "HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning," *Sensors*, vol. 23, no. 18, 2023, doi: 10.3390/s23187856.

[23] J. Miller and R. Thomas, "SDN Security: Anomaly Detection Using Ensemble Learning Techniques," *IEEE Access*, vol. 12, pp. 30345–30356, 2024.

[24] S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions," *Int. J. Inf. Manag. Data Insights*, vol. 2, no. 2, p. 100134, 2022, doi: 10.1016/j.jjimei.2022.100134.

[25] D. Williams and A. Brown, "Comparing the Effectiveness of SVM, KNN, and Random Forest for SDN Intrusion Detection," *Journal of Cybersecurity and Privacy*, vol. 3, no. 2, pp. 150–165, 2023.

[26] https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset

[27] M. H. G. Muhammad, R. Ahmad, A. Fatima, A. S. Mohammed, M. A. Raza, and M. A. Khan, "Secure and transparent traffic congestion control system for smart city using a federated learning approach," Int. J. Adv. Appl. Sci., vol. 11, no. 7, pp. 1–10, 2024.

[28] U. Asghar, S. Yousaf, A. Fatima, M. Saleem, M. A. Raza, and T. M. Ghazal, "Toward robust image encryption based on chaos theory and DNA computing," Int. J. Adv. Appl. Sci., vol. 11, no. 6, pp. 128–138, 2024.