MACHINE INTELLIGENCE RESEARCH

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

# A DEEP LEARNING BASED INTRUSION DETECTION SYSTEM FOR HEALTHCARE APPLICATIONS

**Abdullah Saleh Alqahtani[1], Saravanan Pandiaraj[2]**
Affiliation (1,2)
Department of Self-Development Skills, Common First Year Deanship, King Saud University, Riyadh 12373, Saudi Arabia

**Abstract:** The innumerable increase in user information and network traffic in healthcare applications has made it complex, especially for network-intrusion-detection systems (NIDS) to be familiar with and perform well. Therefore, Intrusion Systems are considered pivotal in e-healthcare systems since the medical details of patients should be confidential, precise, and highly secure. Any variations in the original patient record can lead to massive changes or lead to faults in the treatment as well as diagnosis of diseases like brain stroke. Further, most of the existing studies are focused on intrusion-based systems that are trained with outdated records and intrusion-detection repositories that can generate false positives at a higher rate and need to retain the technique from scratch to handle the complexities that persist in new attacks. In the current research, a novel hybrid method has been integrated with the Gated Recurrent Unit (GRU) along with the Ant Colony Optimization (ACO) algorithm for intrusion detection in healthcare applications.  The proposed approach outperforms the existing models by achieving a phenomenal accuracy of 99%.

***Keywords: Gated Recurrent Unit (GRU), healthcare, network security, Ant Colony Optimization (ACO).***

## 1. Introduction

Network Intrusion Recognition (NIR) is considered a challenging process in the current scenario since certain attacks are generated on a daily basis due to frameworks, software, and new technologies. Various attacks on different organizations focused primarily on stealing the user's private information. Certain metrics that have been considered in the research exhibit a vital backdrop that occurred in modern-day cyber-attack prediction as well as prevention. Due to the enhancement in the healthcare industry, hospitals are associated with e-healthcare systems that meet the requirements of the patients'. Therefore, it is significant for hospitals to manage Electronic Health Records (HER) along with Patient Records, which are also known as Personal Health Records (PHR) since the represented details include the complete patient health records, including the treatment and diagnosis information [1] [2]. Various existing types of research are executed with the real-time software used for IDS with the utilization of rule-based approaches such as signature-based detection, statistical packet analysis, and stateful-protocol analysis. Further, Intrusion Detection Process (IDP) is utilized in the existing research to monitor suspicious activities or activities occurring in the network or computer system. The procured results have been analyzed and monitored in an appropriate way to identify suspicious activities intruding on the network and system. Various activities have been reported to the IDS administrator, who decides future events. Existing research utilized Support Vector Machine

(SVM) in malicious traffic classification acquired from the traffic pattern that comes under non-linear patterns [3].

The IDS deployment consists of five types such as Network-based IDS (NIDS), Host-based IDS (HIDS), Protocol-based IDS (PIDS), Application-based IDS (AIDS), and Hybrid- IDS (HyIDS). The explanation of these terms is as follows [13]:

- Network-based IDS (NIDS) - NIDS is an independent platform that identifies malware attacks or intrusions by analyzing and monitoring the system with the hosts and traffic.
- Host-based IDS (HIDS) - HIDS is an agent presented on the host that identifies intrusion by specific monitoring system application calls and logs.
- Protocol-based IDS (PIDS) - Normally, the PIDS is installed on the specific accessible web server for protocol analysis presented in the computer system.
- Application-based IDS (AIDS) - Mainly, AIDS concentrates on specific application protocol monitoring utilized by the computer system.
- Hybrid- IDS (HyIDS) - HyIDS is the association of multiple IDS techniques to formulate a HIDS, where the system information and host agent are utilized to develop the entire network perception.

Moreover, the E-health system has grabbed the researcher's and health industry's attention in the last decade. However, the high throughput in the devices generates the apparent target for malicious cyberattacks. Hence, these scenarios desperately required protection for the system from various attacks. Most of the scientific research presented with an Artificial Intelligence - AI-based SDN - software-denied networking IDS in order to solve the cyber-attacks threats presented in the internet-of-medical-things (IoMT) and E-health system in various environments [4]. Industries are increasingly focused on various studies on attacks and different fields [7], [8], [18] in order to optimize attack detection. The chosen intelligent methods utilized in the research are tested and verified and then compared to the accuracy rates. The existing studies concentrated on rigorous state-of-the-art methods of Machine Learning (ML) methods employed in Intrusion-Detection and Internet-of-Things, especially for computer network security [5], [6]. However, the main limitation of the existing research in the IDS model occurs due to the random behavior and dynamic variations during malicious attacks and scalable solution design that has the capability to manage this behavior.

Furthermore, the prompt variations in the rapid development and network behavior of various attacks executed the way for estimating different datasets developed over the years and formulating various dynamic techniques. Various unsupervised and supervised ML tools are efficiently initialized for certain purposes in the healthcare industry. Therefore, the techniques used in the existing research include compacted hybrid Methods, Decision Jungle (DJ), Decision Forest (DF), Decision Tree (DT), Random Forest (RF), Naive Bayes (NB), Genetic Algorithm (GA), Hidden-Markov Model (HMM), Logistic Regression (LR), Artificial Neural Network (ANN), Support-Vector Machine (SVM), and Fuzzy Logic (FL) [10], [11].

Despite various existing types of research that concentrated on intrusion detection issues, the existing models implemented different shortcomings. For instance, this research does not concentrate on the class imbalance problems often encountered in ID datasets. The acquired training sample size was chosen randomly compared to a systematic method. However, these methods are also limited by using outdated datasets that include NLS-KDD99. Further, the outcomes reported are generally only processed utilizing one dataset compared to the validated utilizing multiple datasets. Hence, these researchers examined the hyper-parameter optimization utilizing different methods and used certain techniques instead. Likewise, only a few studies studied the existing technique's time complexity and an often unmarked measure [12].

The main contribution of this paper are as follows:

- An optimized Gated Recurrent Unit (GRU) is proposed in this paper for detecting intrusions in smart healthcare applications.
- A distributed dataset is used in this research to analyze unauthorized intrusions based on the collected attack-related data. The algorithm is used to classify the traffic with high classification accuracy and lower error rates.
- The proposed approach is designed based on a feature selection and classification mechanism to enhance the accuracy of attack detection.
- The proposed attack detection model monitors the network traffic continuously and identifies suspicious activities with the traffic at early stages of the attack.

The remaining sections are organized as follows: Section 2 discusses the existing literary works based on the security of healthcare applications using IDS. Section 3 illustrates the proposed methodology and briefs the security problems in these systems. Section 4 discusses simulation results and Section 5 is the conclusion of the paper.

## 2. Related Works

There has been a significant interest in the field of intrusion detection in the healthcare domain. Several researchers have proposed different intrusion detection techniques. The authors in [14], an intelligent intrusion-detection method was utilized in the existing research adapted to the IoT environment. Therefore, predicting IoT-system attacks in real time is essential, enabling efficient defense and security. Particularly the utilization of deep-learning methods in the existing research to detect suspicious and malicious activities in IoT networks. The prediction outcome enables the security-as-a-service along with facilitates interoperability amidst different network communication protocols utilized in IoT. The detection framework has been evaluated utilizing real-network traces, enabling a proof-of-concept. Further, utilizing the simulation process for enhancing the scalability. It is denoted that used IDS was tested and trained against certain testing datasets. Nevertheless, if the testing prediction does not match the outcomes procured from the testing dataset, the process executed in the system combines the training and testing datasets and re-trains with the help of cross-validation.

In [15], an IDS - Intrusion-detection system was utilized for IoT-network that has the capability to predict different attacks in accordance with the hybrid CNN -c convolutional-neural-network model. Nevertheless, IoT enables various services via applications, it encounters severe security problems, and most of the time, it is vulnerable to certain attacks, including denial-of-service attacks, eavesdropping, sinkhole attacks, etc. Hence, IDS was utilized to detect certain attacks during the breaching of network security. This method was adequate for a broad choice of IoT applications, and the technique was validated and compared with techniques such as conventional ML and DL models. During the experimentation process, this technique was more sensitive to malicious attacks, especially in the IoT network. Certain parameters that include precision and recall are the same as Recurrent Neural Network (RNN). Nevertheless, the false positive and true positive ratio was more effective than the RNN model.

In [16], the IDS mechanism was developed to predict intrusion at various stages. The existing research focused on improving IDS by utilizing rule-based and learning-based intrusion classification and detection methods. In a real-time scenario, the intrusion is considered a massive threat to unauthorized information leveraging valid network or user identities and vulnerabilities. Different algorithms such as SVM, RF, and NN can also be used in the existing research; the outcome procured from Ml-based and rule-based methods are evaluated utilizing a regular dataset that includes kddcup-99. SVM was procured with the best result in accuracy compared to other techniques. Also, SVM procured efficient results compared to the RF and NN. The issues due to the network's vulnerability and the host's illegal operations have to be noted in the current environment. Finding effective techniques for security vulnerabilities on monitoring, identifying attacking trends, and much more is significant. Existing IDS systems are procuring the maximum number of false alarms.

In [17], an intelligent and effective NIDS-based DL method was utilized in the research for various tasks, such as identifying and detecting malware. It is essential to shift the real-world process to the cyber environment in a practical way because of the communication that happens over the internet. Due to the rising number of vulnerabilities and attacks, security plays a significant role in computer systems. In most scenarios, network administrators are less likely to secure the networks from cyberattacks. To tackle these security difficulties, various methods were developed for NID. However, various challenges have been faced due to the development of new vulnerabilities by intruders that current devices cannot comprehend. The DL-based IDS method for attack detection was trained with the datasets in real-time and procured with an accuracy rate of 100% and 99.64% in training and testing with the real-time datasets. Eventually, RNN was considered a proficient method, especially for managing the sequence of data. Nevertheless, still gradient loss. Long-term reliance and gradient growth problems occurred in the training process.

In [19], a DL-based ID paradigm was utilized in the IIoT with hybrid methods that define rule-based feature-selection methods for training purposes and verify the provided data captured from the network system. Therefore, NIDSs were developed to secure the system. However, the data collection in the research was utilized in intelligent NIDS development, which was considered a complex task. Also, there are serious limitations in identifying new and existing attacks. Further, the training process in the research was investigated utilizing a deep feed-forward neural network model and hybrid rule-based feature selection. The datasets used in the research are UNSWNB15 and NSL-KDD for testing with the utilized technique and procured in terms of FPR, detection rate, and accuracy by 1.0%, 99.0%, and 99.0%, respectively, for the dataset as mentioned earlier.

In [20], FIDChain-IDS was utilized in the research with the lightweight Artificial-Neural-Networks (ANN) in the way of Federated learning (FL) to enhance the preservation of healthcare data privacy along with the blockchain technology advancement that enables a distributed ledger for accumulating the local weights and then stated the global weight that is updated after averaging, that prevents from certain attacks and enables the immutability and transparency over the certain transmitted system with insignificance overhead. Finally, the procured results exhibited that the ANN models with effective performance and higher accuracy with the data heterogeneity in IoT devices that includes intensive care unit (ICU) in the healthcare industry. In the evaluation process, the CICIDS2017 dataset was procured with 97% accuracy, which is lower when compared to the FISChain. However, most of the time, it eradicates the centralized server, which results in no update when it comes to the global-model weights.

## 3. Proposed IDS Approach

This research implements a Gated Recurrent Unit (GRU) algorithm for the detection of unauthorized intrusions in smart healthcare applications. The proposed attack detection approach will be designed based on feature selection and classification mechanism. The selection of appropriate numbers of features reduces the execution time of the GRU algorithm and improves the attack detection accuracy. The inclusion of redundant and inappropriate features affects the computational performance and increases detection time. In addition, the irrelevant features will have a negative impact on the attack detection accuracy. Hence, it is important to select only relevant features to maximize the computational performance of the ML approach. Here, the features are selected for each specific type of attack and the selected features are used to train the GRU classifier for intrusion detection.

### 3.1 Data Collection

The data for the experimental analysis of the attack detection approach is obtained from the UNSW-NB15 attack detection dataset. The UNSW-NB15 dataset is a publicly available dataset which has 2.5 million records of different attack related data. The data in this dataset consists of both normal and attack samples and all the data is labeled into the respective category. The UNSW-NB15 is a recently developed dataset which also incorporates new and recent attack samples. As a result, this dataset is profoundly used to train ML and DL classifiers for detecting intrusions. In addition, the number of redundant attack samples is comparatively less in UNSW-NB15 compared to NSL-KDD dataset.

### 3.2 Data Preprocessing

Preprocessing is performed to make the data suitable for classification purposes. In this stage, the data collected from the dataset is preprocessed to filter out uncertainties such as missing data, and highly correlated features. These uncertainties have to be removed in order to improve the classification and attack detection performance. The UNSW-NB15 dataset includes attack related features which are used for the classification of attacks for the identification of intrusions. From the available set of attributes, only the selected features such as protocol type, service and flag are converted into numeric features.. These features are transformed into numeric types since the GRU algorithm uses a numeric matrix form to represent the feature vectors. When the algorithm finds the missing data i.e., when the data column is empty, the algorithm automatically detects it and removes the entire data column. In another step of preprocessing, highly correlated features are removed since it requires more memory space and also affects the execution speed of the algorithm. The attack related features are measured in terms of their relevance and if two features have a similar correlation score then only one feature is selected and the other one is discarded to overcome the problem of multicollinearity. Further, the data is split into training and testing data wherein the former one is used to train and fit the GRU algorithm and the testing subset is used to evaluate and validate the performance of the GRU algorithm.

### 3.3 Feature Extraction:

The selection and extraction of important and relevant features holds a greater significance to enhance the classification performance. Extraction of prominent attack related features helps in training the model to detect and classify a particular type of attack. In this stage, the significance of each feature is measured and based on the measurement score the features are extracted and are used as input to the classifier. Extraction of only relevant features reduces the computational complexity of the model and results in a smaller generalization error, which is mainly caused due to the presence of redundant features in the dataset. In this research, the selected features are given to the GRU model based on which the data is classified as ‘normal’ or ‘attack’.

### 3.4 Intrusion Detection using GRU

The intrusions will be classified and detected using an optimized GRU model wherein the performance of the GRU algorithm is optimized using an ACO algorithm.

#### *3.4.1 Gated Recurrent Unit*

GRU belongs to the class of recurrent neural networks (RNN) with a gating mechanism. In general neural networks process inputs and outputs independently, which is practically not feasible in certain sequential processes. RNNs make use of long sequences of information in order to record detailed information. However, RNNs suffer from the issue of vanishing gradient and gradient exploding which affects their performance. To overcome this problem, advanced variants of RNN such as Long Short Term Memory (LSTM) and GRU are introduced. LSTM models can solve problems in applications that depend on the information about previous sequences such as speech recognition, sentiment analysis etc. Because of its ability to remember long sequence data, LSTM models are used to process sequential data of varying length and to capture long-term dependencies. However, sufficient data is required to train the LSTM model for performing real-time tasks. It is challenging to aggregate such large scale labeled data and this restricts the performance of LSTM models. GRU exhibits better performance in such cases, wherein it is difficult to obtain sufficient labeled data. Introduced in 2014, GRU is considered as an advanced version of LSTM, which possesses similar characteristics. In comparison to LSTM in terms of sequence modeling, GRU requires fewer parameters and hence it is easier to train the model. Unlike the LSTM model, GRU has only three gates without any internal cell state. The

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

data stored in the internal cell state in the LSTM model is embedded into the hidden state of the GRU and this data is forwarded to the next layer and so on. The two main gates of GRU are; an update gate (z), a reset gate (r). In addition to these two, a current memory gate ($\hat{h}_t$) is also included (based on the requirement) which are discussed as follows:

***(i) Update Gate (z):*** The update gate measures the amount of past information which needs to be forwarded into the future layers. It is similar to the output gate in the LSTM models.

***(ii) Reset Gate (r):*** Reset gate measures the amount of past information to forget. The mechanism of the reset gate is the same as the operation of the input gate and the forget gate in the LSTM model.

***(iii) Current Memory Gate ($\hat{h}_t$):*** The current memory gate is usually unnoticed or missed during the execution of GRU. The memory gate is incorporated into the reset gate which is similar to the incorporation of input modulation gate into the input gate. This is done to introduce nonlinearity into the input and make the input zero mean. Another important fact of incorporating the memory gate into the reset gate is to minimize the influence of previous information on the current state which is being forwarded to the next gates.

As discussed previously, the process involved in GRU is the same as that of the fundamental RNN. However, the difference between GRU and RNN is the mechanism of internal operation within each unit as GRU consists of gates that control the flow of information between current input and the previous hidden state. Considering the feasible attributes of GRU, this research emphasizes the implementation of GRU for designing the IDS framework, wherein it is trained to extract features and learn data representations without requiring any domain knowledge.

In GRU, the inputs are considered to be in the hidden state $h_{t-1}$ for previous time instance t-1 and the data $x_t$ at the current time instant 't' with the output $h_t$. The output depends on the previous value of $h_{t-1}$ and the flow of information is controlled by the update and reset gate. The equation representing the function of GRU is given as follows:

$$z_t = \sigma\ (W_z x_t + U_z\ h_{t-1} + b_z),\ \ldots.\ (1)$$

$$r_t = \sigma\ (W_z x_t + U_r\ h_{t-1} + b_r),\ \ldots.\ (2)$$

$$\hat{h}_t = \tanh\ (W_h x_t + U_h\ h_{t-1} + b_h),\ \ldots.(3)$$

$$h_t = (1 - z_t)*\ h_{t-1} + z_t\ *\ h_t\ \ldots.\ (4)$$

Where, σ represents the sigmoid activation function, $W_z$, $U_z$, $W_r$, $U_r$, $W_h$ and $U_h$ are defined as the shared weight matrices which are learned during the training process. The terms $b_z$, $b_r$, and $b_h$ are the learnable biases. The optimization of the model is discussed in the next section.

### *3.4.2 Optimization of GRU using ACO algorithm*

The main objective behind selecting the ACO algorithm is to reduce the computational burden and improve the classification accuracy by extracting relevant features from the dataset. In addition to feature extraction, the algorithm will also optimize the GRU model by tuning the parameters to perform attack detection. When used for optimization purposes, the ACO algorithm will search for an optimal solution to improve the accuracy and convergence speed for optimization. In ACO each population member represents the current best solution for each sub problem, and each sub problem will be solved optimally using the solutions obtained from the iterative process of ACO. In this research, the ACO algorithm will serve multiple objectives. The ACO algorithm will segment (decomposes) a multi objective problem into several single-objective subproblems using an aggregation function and also simultaneously optimizes the problem. In this way the algorithm will reduce the computational burden and improve the convergence and execution speed in robots, which is one of the important criterias required in the attack detection process.

## 4. Results and Discussion

The GRU model is designed to enhance the intrusion detection process. As discussed in the research methodology section, the proposed model can detect intrusions with controlled performance in the presence of attacks.

### 4.1 Dataset Description

The data samples for intrusion detection are collected from the UNSW-NB15 dataset. The performance of the classifier is evaluated with respect to its ability to classify and distinguish between normal and malicious samples. The data consists of both malicious and normal data and the same is used for both training and testing the performance of the model. The splitting of data is shown in figure 4.1.

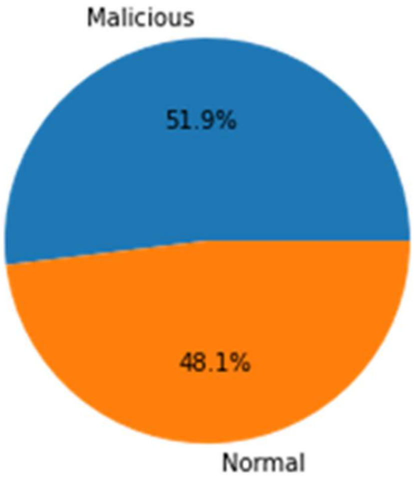
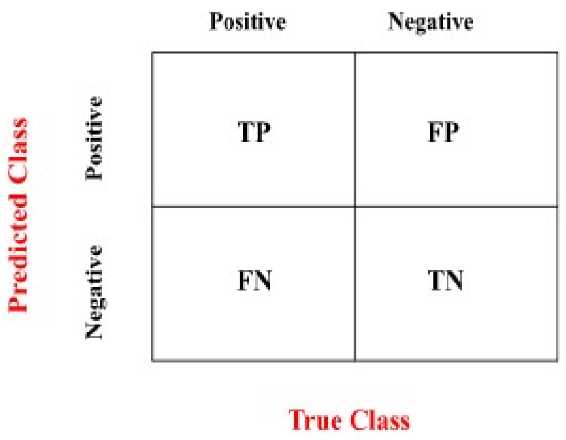


Figure 4.1 Percentage of data split as malicious and normal data

### 4.2 Performance Evaluation

The performance of the proposed GRU based IDS model is evaluated using different evaluation metrics such as accuracy, precision, recall, and F1 score. These elements are measured using the elements such as True positives (TP), True negatives (TN), False positives (FP), False negatives (FN) which are the components of the confusion matrix. In a confusion matrix the output can be two or more classes and it helps to arrive at an appropriate solution by comparing the obtained value (predicted output) with the actual value (ground truth). The confusion matrix is shown in figure 4.2:



| Predicted Class | | True Class: Positive | True Class: Negative |
|---|---|---|---|
| | Positive | TP | FP |
| | Negative | FN | TN |

Figure 4.2 Confusion matrix

Accuracy defines the percentage of number of correctly identified attacks which is defined in the below equation:

$$\boldsymbol{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \ldots . (5)$$

Recall for a function is determined as the ratio of the security attacks that are accurately classified and is given as:

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \ldots .. (6)$$

F1 score is used for measuring the accuracy of the system which can possess the values between 1 and 0. Where 1 represents the best value and 0 represents the worst value. Correspondingly, F1 score is defined as:

$$\boldsymbol{F1\ score} = \frac{\boldsymbol{2 * Precision * Recall}}{\boldsymbol{Precision + Recall}} \ldots . (7)$$

Precision is defined as the number of accurate positive predictions. It is calculated as the fraction of accurately classified network attacks to all other attacks. It is defined as:

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \ldots . (8)$$

The confusion matrix for the proposed attack detection is shown in table 1

Table 1. Confusion Matrix

| **Sample Class** | | **Predicted** | |
|---|---|---|---|
| | | Normal | Attack |
| Real | Normal | TP | FP |
| | Attack | FN | TN |

The classification data for intrusion detection is illustrated in table 2.

Table 2. Classification report of the proposed IDS using GRU

| **No of samples** | **Precision** | **Recall** | **F1- score** | **Support** |
|---|---|---|---|---|
| 0 | 0.00 | 0.00 | 0.00 | 2 |
| 1 | 0.95 | 1.00 | 0.97 | 494 |
| 2 | 1.00 | 1.00 | 1.00 | 31954 |
| 3 | 1.00 | 1.00 | 1.00 | 2594 |
| 4 | 0.25 | 0.50 | 0.33 | 2 |
| 5 | 0.98 | 0.94 | 0.96 | 1368 |
| 6 | 0.99 | 0.89 | 0.93 | 1428 |
| 7 | 1.00 | 0.81 | 0.89 | 2005 |
| 8 | 1.00 | 0.75 | 0.86 | 4 |
| 9 | 0.80 | 0.89 | 0.84 | 9 |
| 10 | 1.00 | 1.00 | 1.00 | 39797 |
| 11 | 0.70 | 0.99 | 0.82 | 1465 |
| 12 | 0.74 | 0.65 | 0.69 | 371 |
| 13 | 0.00 | 0.00 | 0.00 | 1 |
| 14 | 0.41 | 0.43 | 0.42 | 155 |

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

| | | | | |
|---|---|---|---|---|
| Accuracy | - | - | 0.99 | 81649 |
| Macro Avg | 0.72 | 0.72 | 0.72 | 81649 |
| Weighted Avg | 0.99 | 0.99 | 0.99 | 81649 |

The accuracy achieved by the proposed IDS model is 99.9 % and the mean score is 99.88 %.

Graphically, the variations in the performance metrics with respect to number of samples is illustrated in the below figure:

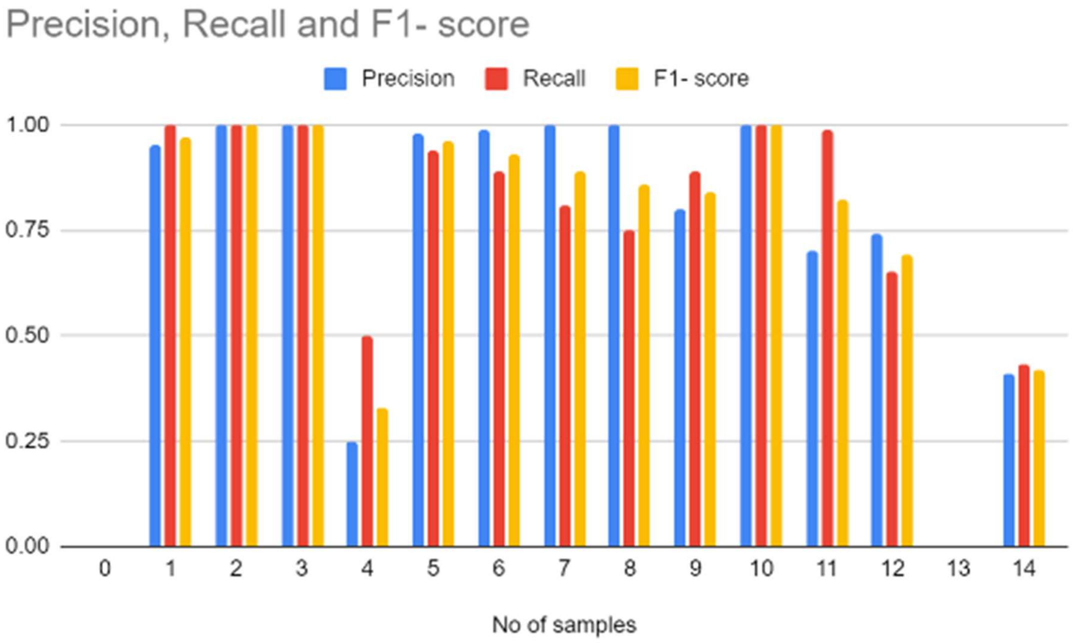


Figure 4.3 Classification of the GRU-based IDS model

### 4.3 Comparative Analysis

In comparative analysis, the results of the proposed GRU model were validated by comparing the results with other existing IDS models such as Random Forest, K-Nearest Neighbor (KNN) and Adaboost classifier. These models have exhibited excellent results in terms of classifying the attacks and hence are mainly selected for the analysis. The classification report and performance of the GRU model and other classifiers are tabulated in table 3.

Table 3. Performance metrics for the classifiers for attack detection

| **Evaluation Metrics** | **Random Forest** | **KNN** | **AdaBoost** | **Proposed GRU** |
|---|---|---|---|---|
| **Accuracy** | 98.01% | 97.55 % | 97.68% | 99% |

| | | | | |
|---|---|---|---|---|
| **Precision** | 97.25% | 96.34 % | 97.87% | 99% |
| **Recall** | 97.28% | 96.28 % | 96.66% | 99% |
| **F1-score** | 95.27% | 94.37 % | 95.76% | 99% |

It can be inferred from the simulation results and the performance evaluation metrics (from table 3) that the proposed GRU model achieves a phenomenal accuracy with respect to different evaluation metrics. The accuracy of the GRU classifier was found to be 99% which is superior compared to existing random forest, KNN and AdaBoost classifiers. Results validate the effectiveness of the proposed attack detection approach.

## 5. Conclusion

This paper evaluated the performance of a GRU-based IDS model for identifying intrusions in smart healthcare applications. The model was trained from the data obtained from the UNSW-NB15 dataset which consisted of attack samples (both normal and malicious). The computational performance of the proposed approach was improved by extracting only relevant attack-related features from the dataset. For intrusion detection, this research employs a GRU model which classified the data type as ‘normal’ or ‘attack’. The performance of the GRU-based IDS was evaluated in terms of different evaluation metrics and the same was validated through comparative analysis. It was observed from the results that the GRU model exhibits an excellent accuracy of 99% compared to other classifiers such as random forest, KNN, and Adaboost. Feature Extraction plays an important role in improving the classification performance, which can be validated from the experimental results.

## References

[1] Lee, J. D., Cha, H. S., Rathore, S., & Park, J. H. (2021). M-IDM: A multi-classification based intrusion detection model in healthcare IoT. *network*, *2*, 4.

[2] Akshay Kumaar, M., Samiayya, D., Vincent, P. M., Srinivasan, K., Chang, C. Y., & Ganesh, H. (2022). A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning. *Frontiers in Public Health*, *9*, 2295.

[3] Begli, M., Derakhshan, F., & Karimipour, H. (2019, August). A layered intrusion detection system for critical infrastructure using machine learning. In *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)* (pp. 120-124). IEEE.

[4] Wahab, F., Zhao, Y., Javeed, D., Al-Adhaileh, M. H., Almaaytah, S. A., Khan, W., ... & Kumar Shah, R. (2022). An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health. *Computational Intelligence and Neuroscience*, *2022*.

[5] Da Costa, K. A., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches.

*Computer Networks*, *151*, 147-157.

[6] Nguyen, P. T., Huynh, V. D. B., Vo, K. D., Phan, P. T., Elhoseny, M., & Le, D. N. (2021). Deep learning based optimal multimodal fusion framework for intrusion detection systems for healthcare data. *CMC-COMPUTERS MATERIALS & CONTINUA*, *66*(3), 2555-2571.

[7] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409.

[8] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors*, *22*(6), 2112.

[9] RM, S. P., Maddikunta, P. K. R., Parimala, M., Koppu, S., Gadekallu, T. R., Chowdhary, C. L., & Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications*, *160*, 139-149.

[10] Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M., ... & Cho, G. H. (2021). Towards machine learning based intrusion detection in IoT networks. *Comput. Mater. Contin*, *69*(2), 1801-1821.

[11] Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. *Engineering, Technology & Applied Science Research*, *11*(4), 7326-7331.

[12] Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2020). Multi-stage optimized machine learning framework for network intrusion detection. *IEEE Transactions on Network and Service Management*, *18*(2), 1803-1816.

[13] Khare, N., Devan, P., Chowdhary, C. L., Bhattacharya, S., Singh, G., Singh, S., & Yoon, B. (2020). Smo-dnn: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. *Electronics*, *9*(4), 692.

[14] Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors*, *19*(9), 1977.

[15] Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, *2*(04), 190-199.

[16] Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, *2*(04), 190-199.

[17] Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, *10*, 100053.

[18] Ullah, S., Khan, M. A., Ahmad, J., Jamal, S. S., e Huma, Z., Hassan, M. T., ... & Buchanan, W. J. (2022). HDL-IDS: A hybrid deep learning architecture for intrusion detection in the internet of vehicles. *Sensors*, *22*(4), 1340.

[19] Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. *Wireless communications and mobile computing*, *2021*, 1-17.

[20] Ashraf, E., Areed, N. F., Salem, H., Abdelhay, E. H., & Farouk, A. (2022, June). Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications. In *Healthcare* (Vol. 10, No. 6, p. 1110). MDPI.