Enhancing Cybersecurity in IoT Healthcare Systems: A CNN-GRU Hybrid Approach for Intrusion Detection

MSc Research Project
MSc In Cyber Security

Ashna Usman
Student ID: 23190264

School of Computing
National College of Ireland

Supervisor: Prof. Niall Heffernan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ashna Usman		
Student ID:	X23190264		
Programme:	MSc in Cyber Security	**Year:**	2024-2025
Module:	MSc Research Project		
Supervisor:	Prof. Niall Heffernan		
Submission Due Date:	12/12/2024		
Project Title:	Enhancing Cybersecurity in IoT Healthcare Systems: A CNN-GRU Hybrid Approach for Intrusion Detection		
Word Count:6892		**Page Count:** 22	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: *Ashna Usman*

Date: 12/12/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Cybersecurity in IoT Healthcare Systems: A CNN-GRU Hybrid Approach for Intrusion Detection

Ashna Usman
X23190264

Abstract

The proliferation of IoT devices has revolutionized industries such as healthcare, smart homes, and manufacturing, but has also made them prime targets for sophisticated intrusion attacks. Traditional intrusion detection methods become inefficient in IoT networks because of the dynamic nature of IoT and due to issues like model shift, problem of generalization and ineffectiveness when dealing with zero-day attacks, etc. To overcome these drawbacks, this research adopts a new approach that involves Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU). It is therefore important to use simple mathematical equations, so that the model that results from this research can be implemented in real-time; preferably in low-powered IoT devices. Using the IoT Healthcare Security Dataset sourced from Kaggle, data preprocessing, normalization, and features extraction were conducted to improve the efficiency of the model proposed. CNN-GRU is computationally efficient and has high detection accuracy and the model can be deployed in real-time in resource-constrained IoT devices. The efficiency of the model is specifically described by 99.52% accuracy, 98.7% precision, 99.6% recall, and 99.49 F1 score of detection. These results place the model to be used as a reference against which future IoT security frameworks become benchmark-able based on the effective approach towards complex IoT intrusion detection that is both scalable and resource-efficient. The proposed CNN-GRU approach outperforms CNN-LSTM (2021), RLSTM (2022) in terms of performance metrics. Despite these benefits it is crucial to perform further validation on different IoT environments and introduce other types of threats to reduce threats to generalizability and make it more flexible

1 Introduction

The development of IoT devices transformed almost all kinds of industries such as health care, manufacturing industries and smart home industries by providing deep interconnectivity of devices. Nevertheless, the rapid growth of online platforms also attracted the increase of threats known as intrusion. Since many IoT devices usually lack adequate security controls, attackers will revel in attempting to gain unauthorized access and control over them. For IoT, which consists of countless evolving systems and devices, detecting and mitigating these threats has become even more important as intrusion sophistication rises. IoT's goal is to integrate practically any physical item into a system of networks Any given physical object that can be turned into a regime of interconnecting networks which data can be retrieved at any time and at anyplace.

Current machine learning (ML) algorithms for IoT security prevention also come with some drawbacks, such as generalization challenges and model shift. Generalization for a model is the capability of the model to extend from training data, and the patterns discovered within, to new, previously unseen states or conditions, including those that are as yet unknown as zero-day attacks. In contrast, model drift can be defined as a situation in which changes in data distribution over different period reduces the efficiency of the model (Vailshery, 2023). Due to the continuous evolvement of threats in IoT environment, the attack strategies and corresponding intrusion like adversarial attacks are introduced which further widen the difference between the data used in the training process. Further, the current research mainly focuses on the middle ad later phases of botnet evolution which, as mentioned earlier, are insufficient when it comes to implementing timely prevention mechanisms during the initial phases of a botnet infection and recovery (Merlino and Allegra, 2024). Smart devices, few computational resources and relatively weak security, are vulnerable to cyber criminals. This places them at high risk of succumbing to spear-phishing, intrusion, keystroke logging, SQL injections, tampering, physical breach, eavesdropping, selective forwarding, man-in-the-middle attacks and network scanning. But this growth comes with its problems such as device management, volume of data generated, and security threats. Past incidents, like the Mirai botnet attack of 2016 showcase that the IoT devices have enormous vulnerability to cybercriminals. Spear-phishing, key logging, injection attacks including SQL injections, man-in-the-middle and many more poses threat to the confidentiality, integrity and availability of IoT systems (Berger, Bürger and Röglinger, 2020). Thus, current IDSs continue to pose challenges to emerging ML approaches; for instance, model drift, which occurs where modifications in data distribution curve over time affect the model's effectiveness(Carter *et al.*, 2022). Moreover, most solutions provided are aimed at the subsequent stages of intrusion detection, while IoT devices are exposed during the first stages of attack phases recovery (Jullian *et al.*, 2023).

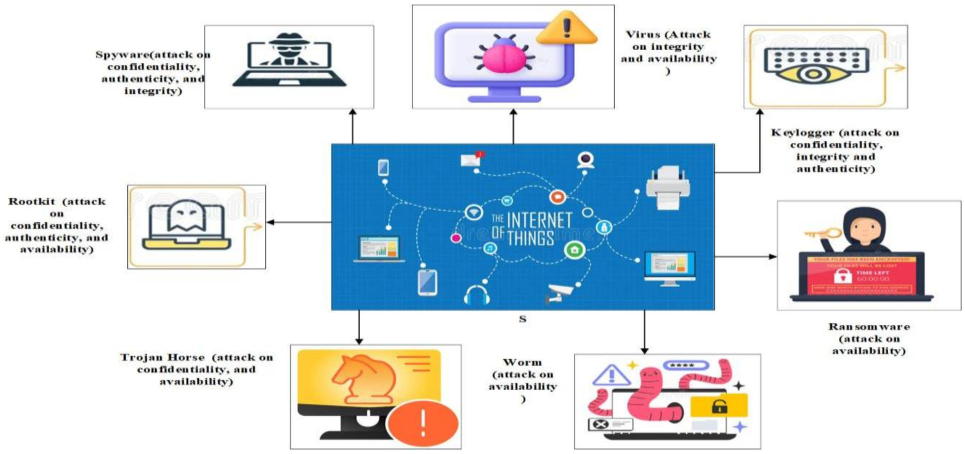
Spyware(attack on confidentiality, authenticity, and integrity)
Virus (Attack on integrity and availability)
Keylogger (attack on confidentiality, integrity and authenticity)
Rootkit (attack on confidentiality, authenticity, and availability)
THE INTERNET OF THINGS
Ransomware (attack on availability)
s
Trojan Horse (attack on confidentiality, and availability)
Worm (attack on availability)

Fig 1: Different types of cybers attacks in IoT environment

This Fig 1. shows various forms of intrusion attack that can be leveraged against IoT gadgets. Different threats are depicted including spyware, rootkits, trojan horses, ransomware, worm, viruses and key loggers as well the impacts on confidentiality, integrity, availability and authenticity.

1.1. Research Question

1) What are the common intrusion threats known to be active against IoT devices, and how do they impact IoT security?

1.2. Objective

1) To identify and forecast intrusion threats with regard to IoT gadgets to determine the effects on confidentiality/ integrity/ availability of IoT security.

1.3. Motivation

The motivation of this study is to address IoT security concerns and design an efficient CNN-GRU architecture for real-time detection with a high accuracy rate for resource-limited gadgets. Applying the proposed model to the IoT Healthcare Security Dataset the model achieves outstanding results. Yet, it is important to note that additional validation across different application contexts is required to expand on its operational utility in other contexts.

1.4. Summary of Content

The proposed study is organized into five sections: Section I is the Introduction, Section II is the Literature Survey, Section III is the Research Methodology, Section IV is explaining the design and Implementation, Section V is stated the Result of the study and Section VI stated the Discussion and Conclusion.

2 Related Work

Alwahedi et al. (2024) providing a comprehensive overview of ML (ML) solution for cyber threat and related topic, approach, and drawback; however, the problem remains open. The paper also describes a brief analogy of the presently evolved IDSs based on ML and outline the open issue in the field which indicates the future direction on IDSs. The survey starts with the situations that IoT devices have become a part of every-day like basis objects that connect and provide comfort to human life while carrying a large number of threats. These are real problems originating from growing interconnected systems that need to be addressed to help IoT networks be safe and reliable. The key parts of the survey contain the information about definitions, attack surfaces and evaluations of recent methods for the cyber threat detection. In conclusion, it is advised recommending urgent and versatile measures and practices for enhancing IoT security which use multiple approaches simultaneously. The current study is in the form of a survey which can act as a reference for carrying out contemporary advancements in the area ‘IoT security’, with recommendations of major hurdles and indications of further research and development in looking to produce a more enclosed IoT environment.

The study discusses and compares existing solutions for IoT cyber threats based on ML, examines approaches to intrusion detection systems, introduces a new type of AI, generative AI, and defines the need for a comprehensive approach towards the unsolved problems of IoT security. I will critically analyse this study by integrating emerging technologies, real-world IDS case studies, advanced ML solutions, and human factors in IoT security

Khan and Alkhathami (2024) employs the IoT dataset from the Canadian Institute for Cybersecurity (CIC) to design ML approaches for proper detection of inefficient traffic in IoT networks. In total, there are 33 type IoT attacks collected in the dataset and divided into seven major classes. For the analysed dataset, Data preprocessing is applied and class distribution is equilibrated when training binary classification Supervised ML models. These models are RF, Adaptive Boosting, Logistic Regression, Perceptron, and Deep Neural Network. The study aims at improving the models by deleting the multicollinearity features, reducing the dimensionality, reducing overlearning and training time to make the models more efficient. Surprisingly, the Random Forest model yielded impressive results and was the most effective for binary and multiclass classification of IoT attacks using both a limited number of and all 187 features available at a record accuracy of 99.55%.

The authors apply and build ML techniques on the CIC IoT dataset for identifying malicious traffic; the authors discuss Risk Issues to Medical IoT devices where the proposed model has an accuracy of 99.55% Random Forest. The following critiques will be made on this study: Dataset strength, measures utilized, feature choice, practical application, and IoT security research improvements.

Qaddos et al. (2024) contributes a new approach on enhancing CNN-GRU based MDL architectures recommended for IoT intrusion detection. Combined learning model performs well in accurately capturing complex patterns and training relational information which is significant in IoT safeguard. In addition, we use the FWSMOTE to tackle the problem of imbalanced datasets, which often occur in intrusion detection scenarios. Exceptional verification is achievable employing the IoTID20 dataset imitating IoT context with the attack detection accuracy of 99.60%, which surpass the previous studies. Similarly, evaluation on the network domain dataset is also promising with 99.16% accuracy of UNSWNB15 dataset making it plausible for any kind of dataset. This is also strong innovatively for today’s IoT intrusion detection and at the same time, it lays a new floor in precision and flexibility. These results evidence its applicability as a robust and flexible approach necessary in protecting IoT environments from emerging threats.

The authors introduce a new hybrid CNN model for IoT intrusion detection performing very high accuracy and flexibility. It brings improvements for imbalanced datasets using FWSMOTE and establishes new state-of-the-art results in IoT security and as a cross-dataset study.

Smart health care devices based on IoT such as Patient Monitoring Cameras in a hospital generate vital information that require a layer of protection against attackers. To protect the billions of records created by the IoT before they are attacked, proper intrusion detection is needed on the personally identifiable information. Jeyanthi and Indrani (2023) suggests the five-layered model to look for an intruder in big data. This work employs the creation of new custom features to make the learning rate even higher and to reduce the restricted kind of perception that the machine model goes through when learning. ACAAS is proposed in IoTID20 for defending IoT networks and for this goal, based on proposed ACAAS, few aspects are derived for detecting the assault for improved prediction. The authors mentioned the Accuracy Rate for current proposed schema at an Error rate of 0.0083% is 99.16%, Sensitivity Ratio 99.89%; Specificity Ratio 98.203% for IOTID20 with some modified features implemented by RNN-BiLSTM. The high accuracy rate thus obtained reveals some realities that the system has the capacity to protect the network against intruders.

The authors pay particular attention to the selection of features that may be unique to IoT environments, the use of a combined RNN-BiLSTM architecture and provide a very extensive analysis based on IoTID20, which demonstrates high accuracy as well as relevance to IoT health care. These ideas support the CNN-GRU model, recommended for the effective implementation of the proposed study.

Alomiri et al. (2024) introduce a Ridge Classifier is employed as a robust classification model for finding out the intrusive in IoT systems. Through implementation of this approach, real-time detection and prediction of cyber-attacks in the network can be easily achieved by the proposed security system due to its access to secure and updated information in the network. The picture further enriches by the integration of the ML techniques which in turn further helps the system to identify and neutralize threats efficiently. It is also demonstrated experimentally that the proposed system can successfully detect and avoid the threats in IoT systems with a very high accuracy of 97%. Furthermore, the enlisted methods of fortified models and specifications of security all across actually provide a full as well as satisfactory protection against many threats. Second, having agreed with the possibility of using ML to increase security in IoT systems, we corroborate the previous point by showing how Ridge Classifier model can provide the benefits of protection such as IoT systems mentioned above. These measures contribute essentially in providing high level accuracy of threat identification and prevention of the networks and enhance protection of government and business networks. In addition, exposing data in the face of dangerous threats increases the security and privacy of IoT systems, and ensures positive perceptions and utilization in the burgeoning sector of IoT technology.

The authors propose a Ridge Classifier to effectively predict real-time cyber-attacks in IoT systems, achieving 97% accuracy to enhance security. I’ll critically analyse this study by evaluating model strengths, limitations, performance metrics, deployment challenges, and proposing enhancements for IoT cybersecurity.

On one side IoT’s characteristics make it rather easy to implement in actual practice while in return is somewhat very susceptible to cyber risks on the other side. Of all the attacks against IoT include: Denial of Service (DoS) is definitely among one of the worst forms. Verma and Ranga (2020) option to apply the ML classification method to safeguard IoT against DoS attacks. The existing state of intrusive-based intrusion detection systems (IDSs) can be benefited by using the classifiers that have been reviewed in this paper. Methods and approaches applied to validate the classifiers are described according to basic performance characteristics. Three standard classification models are selected; CIDDS-001, UNSW-NB15, and NSL-KDD. Therefore, the specific objectives of this research are to encourage the IoT security researchers for designing IDSs employing ensemble learning technique.

The author discusses the advantages of using ML classifiers in IoT IDS against DoS attacks in terms of statistical analysis, benchmark dataset, and practice using the hardware environment. These insights are useful in the implementation of selection and evaluation of adequate classifiers in the proposed study.

IoT healthcare systems security can be improved by applying the blockchain-supported intrusion detection in order to secure patient records and other identifying data. Thus, incorporating blockchain technology to IDS, it became clear that such integration can provide a more sustainable and reliable protection for IoT healthcare technique. Using this motivation, Alamro et al., (2023) BHS-ALOHDL technique presented enables the IoT devices for health-care sector to send medical data nutritionally and it again also has provision to deny the IOT to intervene into the system. For this purpose, the BHS-ALOHDL technique has ownership of the ALO based feature subset selection (ALO-FSS) system for the generation of a series of feature vectors. This paper narrows our attention to the HDL model as being a cocktail of two learnings; the CNN features and a LSTM model for intrusion detection. In the subsequent part of the manuscript, the proposed BHS-ALOHDL system is experimented on two different datasets and the results of which are then discussed against other models in this chapter BHS-ALOHDL technique has the potential to perform efficiently.

For IoT healthcare, the author designs a blockchain-based intrusion detection system with ALO and HDL – for enhanced detection rates and secure data transfer. The validity of this method shows growth in various algorithms and could use additional examination of the expansion of applying it in the future.

Iwendi et al. (2021) concerned a part of security-intrusion detection systems because many Specifically, in healthcare and the privacy question, web security attacks have been increasing over the last few years. Many intrusion-detection systems being discussed in various studies are employed for identifying the positions of cyber threats in smart healthcare environment as well as for differentiating the NBAs and privacy violation. The research suggested an ML support system using RF and genetic algorithms. Thus, the performance using the genetic algorithm and RF models. Thus, the performance using the genetic algorithm and RF models that. To enhance the function of the approach developed within this work, a WGA and RF were integrated to provide the best function that provided very high detection rates and low FPR. Thus, the performance using the genetic algorithm and RF models that I suggested has resulted in the performance metres as having a detection rate of 98.81% and a false alarm rate of 0.8%. This work pointed out the privacy concern and the issue of authentication in smart healthcare, wireless communication and the privacy that needs to be implemented in the efficient and intelligent Web system. In addition, the effectiveness of each step of the developed algorithm was investigated when using scaling factors to determine the F1-score and precision associated with NSL-KDD and CSE_CIC_ID, IDS2018 datasets.

Feature optimization such as genetic algorithms, detection accuracy which stands at 98.81%, various datasets, and comparison establish the proposed CNN-GRU hybrid model as relevant and robust in intrusion detection in IoT healthcare.

GHEZALA and Radhwane (2024) proposed an integration strategy of one dimensional convolutional neural network (1D- CNN) with Gate Recurrent Unit (GRU) is developed for EEGs analysis. In addition, utilization of this framework is followed by using the CHB-MIT dataset to assess its performance for the classification between these disorders. Furthermore, the obtained results present a higher accuracy to the establish methods of 1D-CNN-GRU and surpass previous investigations. Last of all, this architecture is precise and confirms the effectiveness of the proposed approaches for detecting and predicting epileptic seizures. And Haddy et al., (2020) seeks to demonstrate that the use of both network and biometric metrics as features provide superior classification performance to using only one of the feature types. We have developed an Experimental and Real-time EHMS that captures the patients' biometrics and network flow statistics. The gathered data is then transmitted to a distant server in order to further analyse and make subsequent clinical decisions. The man-in-the-middle cyber-attacks have been employed and the dataset with normal and attack-healthcare records is more than sixteen thousand records has been developed. The system then uses various machine learning techniques for developing and evaluating the set data against these attacks. This again also establishes a 7% to 25% boost in the final performance with this proving the reliability of the proposed system in providing adequate intrusion detections.

The discussed literature indicates that the application of ML and hybrid architectures improve the IoT cybersecurity level. However, the work done in this area does not fully address the issues of expansion of such models and their applicability to different IoT contexts. The study proposed in this paper aims to fill these gaps by utilizing CNN-GRU structures as well as new dataset enhancement approaches. By drawing from the following literature, we lay a foundation of critical parameters and evaluation strategies instrumental in the successful implementation of the proposed intrusion detection framework early on.

3 Research Methodology

CNN-GRU is the most preferable model for IoT intrusion detection, as it steps simultaneously spatial and temporal data which is essential for analysing intrusion patterns IoT environment. The CNN part extracts spatial characteristics by detecting local patterns in network traffic, system calls or a packet structure, which contributes to dimensionality reduction for optimization.

3.1. Data Collection

The IoT Healthcare Security Dataset (ICU Healthcare Security Dataset) is a mock ICU with two beds and nine patient monitoring devices, or patient sensors per bed, and a control unit called Bedx-Control-Unit. This setup was proposed to examine security in IoT health care context especially in the intensive care unit. the Bedx-Control-Unit is to process the data received further and send the same. The data set comprises normal and adversarial traffic and is compatible with normal IoT operating patterns and possible security threats in an ICU.

Assembled and shared on Kaggle, such data set is helpful for exploring secure IoT healthcare systems (Malik, 2022).

3.2. Data Preprocessing

Consequently, data processing is a paramount phase in the proposed study of IoT-based ICU healthcare security for accurate detection using CNN-GRU. Well-known data processing stages can be described in the following way.

3.3. Normalization

Normalization rescales the data so that ranges of input features have equal affect in the model; it is set usually to range between 0 and 1. The process starts by determining the feasible range for each feature that includes the minimum value and the maximum value then ends up using the equation (1),

$$X_{normalizatin} = \frac{X - X_{minimum}}{X_{maximum} - X_{minimum}} \qquad (1)$$

This kind of data leads to increased learning convergence and reduces chances of being trapped in local optima, which is locally optimal; this is good for processing IoT data with a broad range of sensor data to enhance efficiency in learning and also improving on the model's accuracy.

3.3.1. Data Cleaning

Deals with any discrepancies and errors in the data is the first step. This involves remove the items with significant missing data or addressing missing values using imputed techniques. Consider that the X_c represents a data point with a missing value, it can be imputed using the mean μ of the available data points which is given in eqn. (2):

$$X_c = \frac{\sum_{j=1}^{n} X_j}{n} \qquad (2)$$

4 Design Specification

The design specification that may outline the CNN-GRU intrusion detection system for IoT security that may combine with CNNs for spatial feature extraction and GRUs for temporal pattern analysis. Visualization tools, including graphical representations and confusion matrices, aid in interpreting results. The system uses TensorFlow and Keras, implemented on GPU-enabled hardware via Jupyter Notebook for optimal performance

4.1. Modelling

The system's centrepieces are a model involving CNNs and recurrent neural networks with gates (GRUs). CNNs are used to extract spatial features from the pre-processed sensor data and detect anomalies or outliers in data. The GRU layers then take care of the temporal dependencies hence the system is able to notice slow changes that may be associated with security menace. TensorFlow and Keras tools are used for creating and training of the model, and GPU for boosting computations. Indeed, it is categorized into normal or intrusive through a SoftMax layer, and common means such as precision, accuracy, and F1-score are calculated.

4.2. Visualization

The performance of model and its standards is depicted in graphical form as well as the confusion charts to make the students understand what kind of predictions the system is likely to make.

4.3. Software And Hardware Pre-requisite

Dataset	IoT sensor data from healthcare devices
Hardware	High-performance machine with GPU (12 GB DDR4 RAM recommended)
Software	Jupyter NoteBook with Python, TensorFlow, Keras
Activation Function	ReLU, Softmax
Training Frameworks	TensorFlow, Keras

5 Implementation

The implementation specification describes the CNN-GRU workflow, where IoT data is pre-processed through normalization and cleaning. CNN layers extract spatial features, and GRU layers analyse temporal patterns, creating a detailed feature map. A SoftMax layer classifies the data as intrusion or benign, evaluated using metrics like accuracy and F1-score.

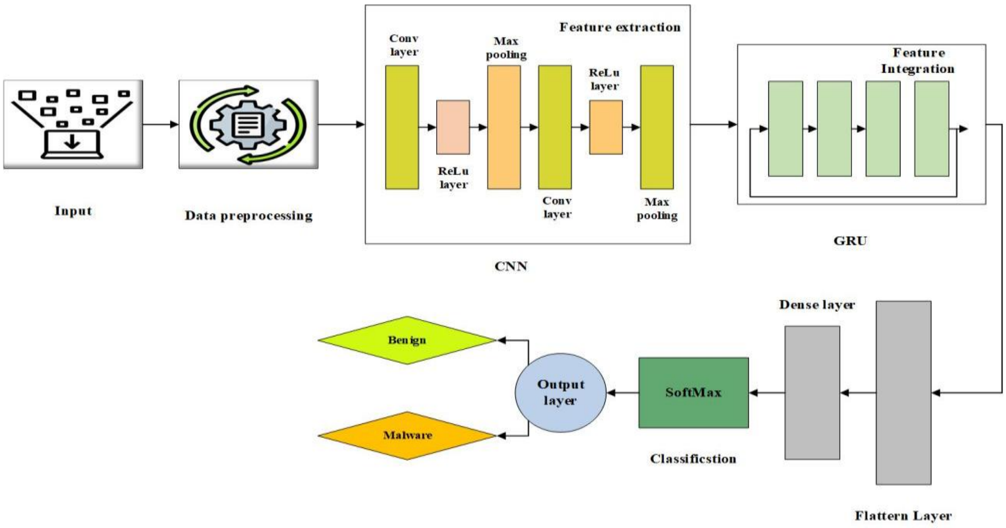

Fig 2. Architecture of CNN-GRU

Fig 2. Present the workflow of the CNN-GRU approach. The IoT data preprocessing is utilized in the proposed study and CNN features incorporate spatial hierarchies such as convolution, ReLU, and max-pooling. The extracted features are then passed through GRU layers to incorporate temporal dependencies as these layers are efficient in that context. The GRU output is flattened and fed to dense layers and SoftMax layer to make final classification and the final layer highlights whether the data is Benign or Intrusion.

5.1 Feature Extraction Utilizing CNN

The feature extraction is the crucial step in this approach which makes use of the features of Convolutional. CNNs for the detection of the underlying framework of the patterns from the input data, which is primarily derived from IoT devices in healthcare settings (Xie *et al.*, 2022).

The actual study under consideration applies CNN to process data from, IoT healthcare devices denoted as a multi-dimensional array shown in the equation (3)

$$X \in \mathbb{R}^{H \times W} \tag{3}$$

where, H and W signifying the height and width of the input data respectively. In convolution operation the use of filters also known as kernels is learnt for local feature representation as given in the equation (4).

$$K[i.j] = (X * L)[i,j] = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} X[i+m, j+n] \cdot Q[m,n] \tag{4}$$

where, Q is the output feature map and Kis the kernel of size m, n. After passing through convolution a non-linear activation function like ReLU is applied to add non-linearity obtained in equation (5)

$$ReLU(y) = \max(0, y) \tag{5}$$

The subsequently, a pooling layer (e.g., max pooling) is adopted to down sample the feature maps, preserve important features described in equation (6)

$$Y_{pool}[j,j] = max_{m,n} Y[i+m, j+n] \tag{6}$$

This makes the final representations smaller high level feature maps which encode important distinction between normal and intrusive behaviours. Lastly, the feature maps undergo dimensionality reduction, slicing in one dimension to form a vector before being fed into the classification stage including, GRU. On the whole, the proposed study of feature extraction in this paper provides a collection of exhaustive approaches for embedding a significant amount of information from input data, which will lead to the increased effectiveness in identifying the presence of intrusion within the IoT operating in healthcare facilities.

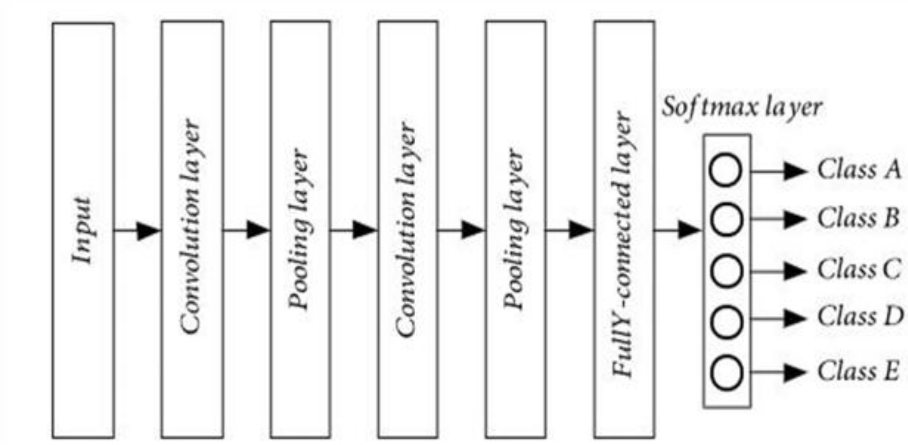

Fig 3. Architecture of CNN

Fig 3. shows the architecture of CNN. For the input data, a set of filters or, more correctly, the list of filters called convolutional kernels is employed. During the design of a map function, each filter glides across the input data. All the above feature vectors are accumulated, meaning that convolution layer has the maximum performance. Freshly Pooling layer, the subsamples on the image reduce the dimensionality of map function. Pooling is most frequently used in two ways: There are two types of pooling; average pooling and maximal pooling. The result of the previous layer becomes the input to the next level which is a single value or vector.

5.2 Feature Integration Using GRU

The operation of feature integration using a GRU enables temporal structure to be learned in an effective manner and the temporal dependencies which are inherent to time-stamped data in IoT and other time-series applications are thereby harnessed (Ravi, Chaganti and Alazab, 2022).

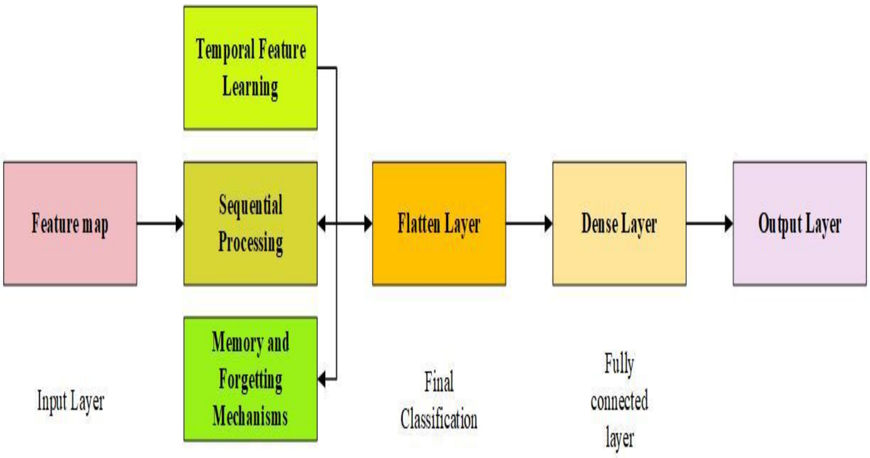

Fig 4. Workflow of GRU

In the following, we illustrated the workflow of the proposed GRU model in detail, and it can be seen in Fig 3.2. CNN feature extraction is initial steps to feed analysed data, for instance, traffic sequences to the convolutional layers that involve filters to look for elementary features such as edges. The obtained feature maps are then followed by ReLU activation function to incorporate non-linearity in the model for learning nonlinear characteristics for complexity. The max pooling layers then down sample these maps, to decrease dimensionality and the amount of computation required keeping only the most important features. It is accomplished through repeated instances of these layers which in turn enables the learning of features, simple and complex within a hierarchical manner. The last encoder-decoder phase features maps are the last high level spatial information which will be later exploited by the temporal component, namely the GRU.

GRU also adopts decoupling routines to manage information exchanges; a problem There are two types of RNN, traditional and recurrent, but the traditional one come with a number of issues of which the most important one is gradient vanishing. This via the Update Gate (u_t) sets up an equivalence between the ratio of old and new information, calculated by the equation (7),

$$u_t = \sigma(W_u \cdot [h_{t-1}, x_t]) \tag{7}$$

while the Reset Gate (r_t) controls how much past information to forget illustrate in equation (8),

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \tag{8}$$

The Candidate Hidden State $\widetilde{h_t}$ is new information made from the current input and the previous hidden state weighted by the reset gate obtained in equation (9).

$$\widetilde{h_t} = \tanh\left(W_h \cdot [r_t \cdot h_{t-1}, x_t]\right) \tag{9}$$

The final feature vector is then taken to a fully connected layer followed by a softmax layer for classification. Inclusion of spatial and temporal features in this approach affords the model the capability to provide qualitatively good forecasts on multiple fronts across data complexity.

5.3 Classification

In the proposed study SoftMax is significantly important in classification because it interprets the final output of the developed MDL model while at the same time providing the probability of each class or category (Chaganti, Ravi and Pham, 2022a). The final hidden state h_t encapsulates essential spatial and temporal patterns, forming a comprehensive feature representative maintains spatial-temporal features after feature extraction through the CNN part and graph reasoning through CNN and GRU (or CNN-Transformer) layers. Because these are all related to each other, the hidden state is then passed fully connected layer that shaves off the last layer of the features and produces the logits or the raw prediction scores. SoftMax then convert these logits into class probabilities while adding them up to get a total of one. So given an input Y across w n classes the SoftMax function computes the probability density of a class and assigns the instance to the class with the highest probability density. In binary classification which is used in detecting between intrusion and benign code. This probability-based output also shows the degree of certainty of the model, a very important feature in many critical real-world applications including intrusion detection or health diagnosis. Metrics for example accuracy, precision, and recall are derived from the SoftMax values that provide details of the relative model's performance with the training and test set.

Lastly, SoftMax maps integrated features into prediction probabilities improving both the classification's precision and probability.

Algorithm 1: CNN-GRU with Fully Connected Layer for Intrusion Detection in IoT Data

```
Output: Classification of IoT data as intrusion or benign
Load the labelled IoT dataset
Normalize the raw data
Segment the data into sequences
CNN Feature Extraction Loop
    while True:
        Pass each data sequence through a CNN layer
        Apply convolution and pooling layers to extract spatial features from each sequence
        Check for feature extraction improvements
GRU Feature Integration
    Input CNN-extracted features into the GRU model
    Compute Update Gate, $u_t = \sigma(W_u \cdot [h_{t-1}, x_t])$
    Compute Reset Gate, $r_t = \sigma(W_r \cdot [h_{t-1}, x_t])$
    Candidate Hidden State Calculation, $\widetilde{h_t} = \tanh\,(W_h \cdot [r_t \cdot h_{t-1}, x_t])$
 If GRU feature integration is successful
        Pass final hidden state to classification layer
Classification Layer
        Feed final hidden state into a fully connected layer
        Classify training set values using SoftMax
          assess training and testing datasets;
   Determine the errors;
producing accuracy reports and graphs;
   if Stopping criteria are met:
        break;
```

6 Evaluation

In this paper, the conceptualisation of an IoT intrusion detection system using an CNN-GRU model for healthcare environment is divided into three phases.

6.1 Performance Metrics- Proposed Method

The performance of the model is measured using the following metrics:

6.1.1 Accuracy

The accuracy is the ratio of well-defined samples or the combining count of the items categorised to the complete number or frequency. When a dataset is balanced it is called Detection Accuracy and can be used to explain how the system is discriminating.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{10}$$

6.1.2 Precision

Precision evaluating the performance In particular, when the false positive rate is relatively costly, one should apply precision evaluating the performance of a classification model. It reflects the number of events labeled as positive (for instance, an “attack” in the sphere of intrusion detection) to actually positive.

$$Precision = \frac{TP}{TP+FF} \tag{11}$$

6.1.3 Recall

Recall is the percentage of the number of software samples correctly identified as Attacks to the total number of software samples which were classified as Attacks. Further, that term, shown in the formula for FDR as ‘Detection Rate,’ can also be found.

$$Recall = \frac{FP}{TP+FN} \tag{12}$$

6.1.4 F1 score

The F1 score which is the measure of both precision and recall of one or more combinations of features. In other words, the matrix represents a technique for the assessment of the effectiveness of an identified system which is in terms of the accuracy of that system as well as the recall of the system.

$$F1\ score = 2\left(\frac{Precision \times Recal}{Precision + Recal}\right) \tag{13}$$

Metrics	Values (%)
Accuracy	99.52
Precision	98.7
Recall	99.6
F1 score	99.49

Table 1. Performance Metrics of CNN-GRU

The Table 4.1. shows the CNN-GRU model's performance, achieving 99.52% accuracy, 98.7% precision, 99.6% recall, and a 99.49% F1 score, highlighting its high detection efficiency.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
CNN-LSTM (Sahu *et al.*, 2021)	91.2	90.81	92.7	91.75
RLSTM (Adefemi Alimi *et al.*, 2022)	99.2	98.3	99.6	99.22
CNN-GRU (proposed)	99.52	98.7	99.6	99.49

Table 2. Performance Comparison of CNN-GRU with Existing Models

The table 4.2. compares the performance metrics of CNN-GRU, CNN-LSTM, and RLSTM models, with CNN-GRU achieving the highest accuracy (99.52%) and F1 score (99.49%), indicating superior intrusion detection efficiency.

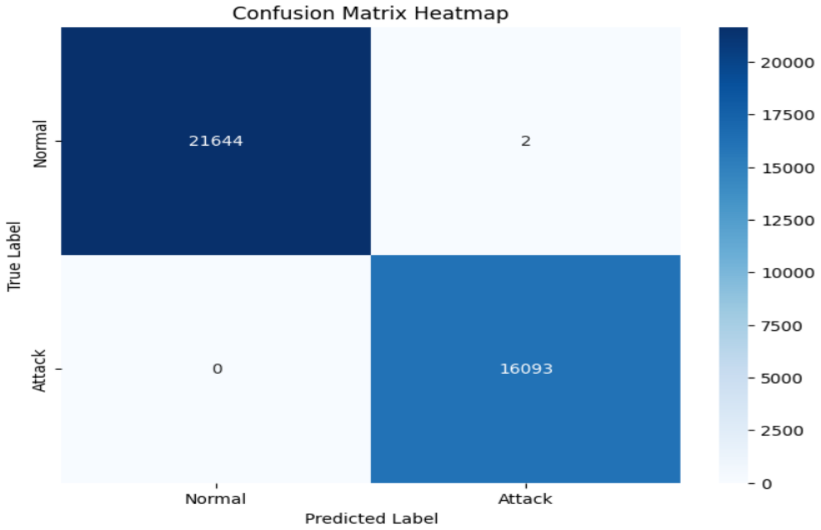

Fig 5. Confusion Matrix Heatmap

In this research, we used the confusion matrix heatmap of classifier performance as depicted by Fig 5. There is the X-axis which represents the predicted labels and Y-axis which represents the true labels; Normal and Attack. In this case there is only 3% misclassification error this means that the model was able to classify well the 21,644 normal and 16,093 attack instances from the datasets with only a small misclassification.

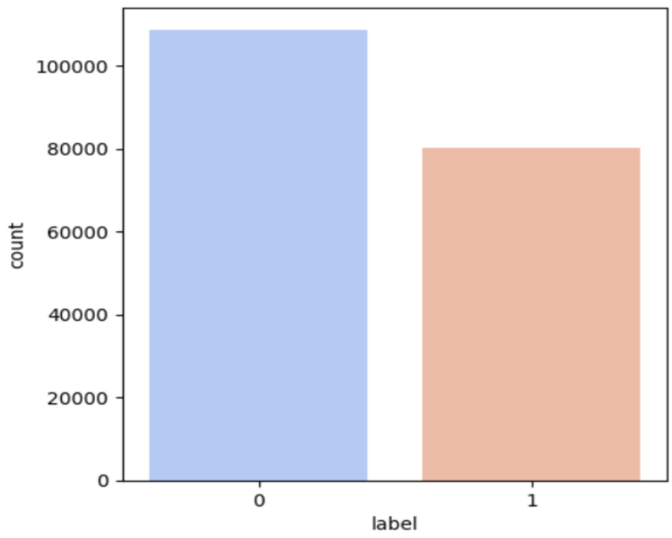

Fig 6. Label distribution within the dataset.

The Fig 6 shows the labels are distributed unevenly within the dataset. Label 0 is used more often, which may signify data inhomogeneity; this problem was solved during pre-processing to make the results more accurate.

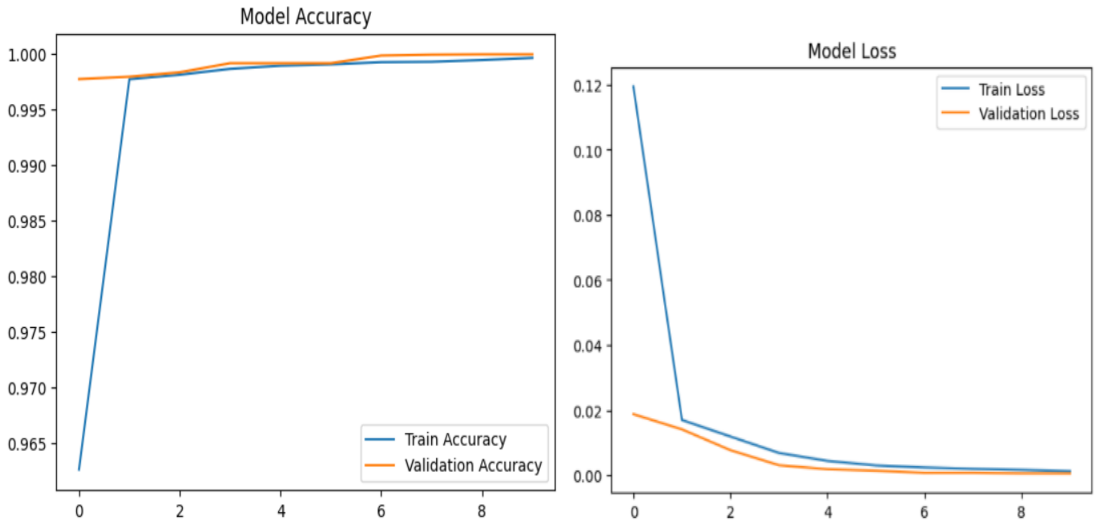

Fig 7. (a). Training and validation accuracy (b) Training and validation loss

Fig 7(a) the training and validation accuracy over epochs in which both of them increased progressively without crossing the threshold of overfitting. The training and validation loss are represented in Fig 7(b), thus ensuring that the model acquires suitable learning with slight overfitting. These trends confirm strong characteristics of the model.

The training and validation accuracy is presented in Fig 7(a), proving a steady increase throughout the epochs and without sign of overfitting.

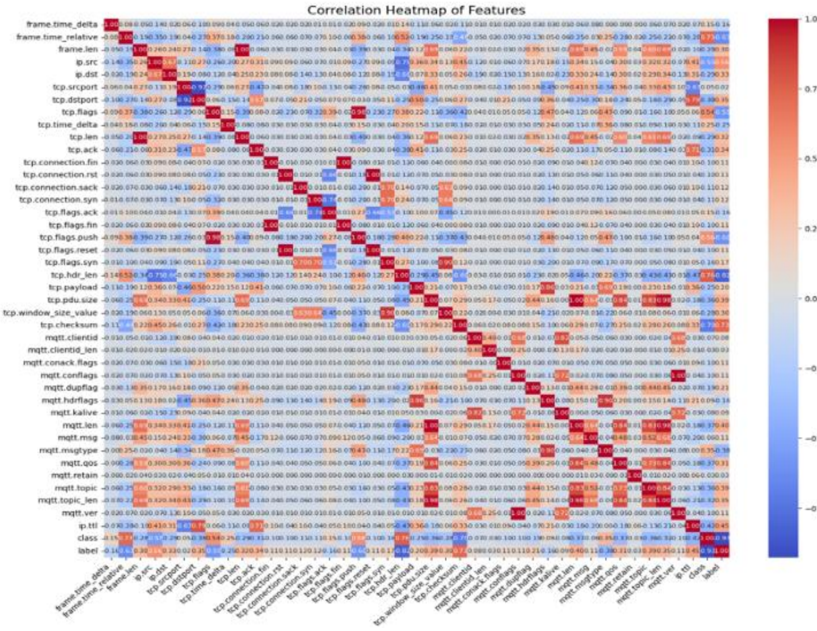

Fig 8. Correlation heatmap of network traffic and MQTT features

The heatmap in Fig 8. shows the association between network traffic and MQTT features. High correlations utilize feature selection and thus allow for input-data culling to be performed.

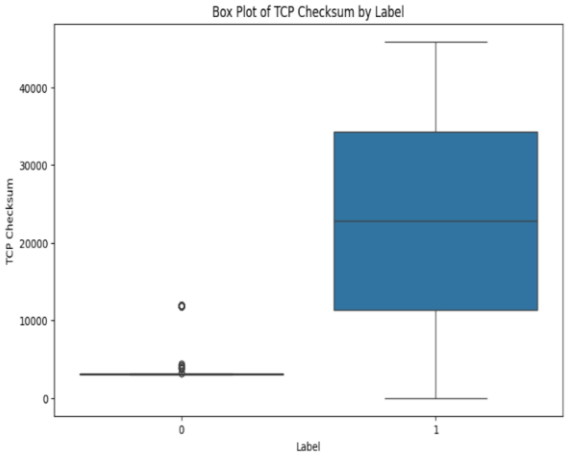

Fig 9. TCP checksum variations by label

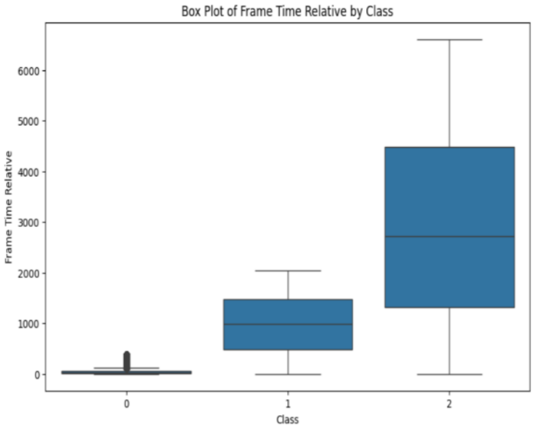

Fig 10. shows frame time relative distributions

Figure 9. represents TCP checksum volatility over time by label and shows that there are differences between labels 0 and 1.

Fig 10. presents frame time in relation to the classes; Class 2 has the greatest variation. These patterns define traffic performance and network configuration

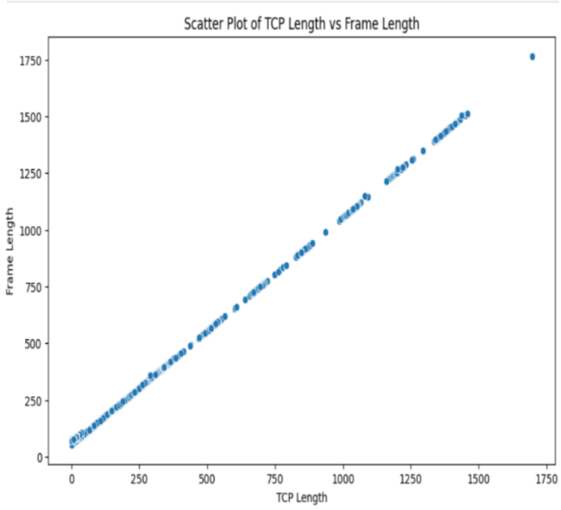

Fig 11. Scatter Plot of TCP length vs Frame length

Fig 11. shows a linear relationship between TCP segment length and total frame length necessary for understanding the protocols and traffic.

6.2 Discussion

This section discusses the CNN- GRU performs in IoT intrusion detection, identifies strengths and weakness of the outlined model, and ends with the possible improvements to IoT security systems in practical scenarios.

The work presented CNN and GRU based model is testified with higher confidence level with accuracy of 99.52%, precision of 98.7% and F1 score of 99.49% which is better in comparison with the state-of-art model such as CNN-LSTM and RLSTM. These metrics substantiate the stability of the model in terms of using the algorithm in detecting intrusion threats to IoT environments. The work done is divided into the following part: designing, implementing, and evaluating the intrusion detection system by applying the CNN-GRU framework. As shown in the experiment with the IoT Healthcare Security Dataset, by utilizing CNN when considering spatial features and GRU for temporal ones, the model allows to address real-world IoT intrusion cases steadily and effectively, the flexibility of this approach is also evident from the nature of the IoT application environments; generalizable to any environment. Nevertheless, future work for robustness should involve the same methodology but performed on other datasets that include encrypted and unbalanced traffic among others.

The main advantages of the approach comprise low computational complexity and the ability to work on resource-limited IoT devices as well as good performance in detecting new attacks. Some of these drawbacks are the use of basic pre-processed data and the requirement of small models suitable for the low-voltage devices. As for further work, the presented challenges should be addressed together with the integration of ensemble approaches for the improvement of IoT security.

7 Conclusion and Future Work

The findings of this particular study are thereby conclusive, that the CNN-GRU model that hybridizes the machine learning along with the deep learning technologies works perfectly well in the identification of intrusion in IoT settings. These findings validate the model's ability to differentiate effectively between benign and intrusive activities, addressing the research question: This raises the question, what the typical intrusive threats recognized to target IoT devices are and how they affect IoT security. However, when comparing our model against other models, our model achieves 99.52 % of accuracies, 98.7 % of precision, 99.6 % of recall and f1 score of 99.49%. This research also fulfils the goal of detecting and predicting intrusion threats in IoT systems as well evaluating their impact on the security of IoT networks. The real-time and accuracy of the proposed model make the model ideal for usage on resource-constrained IoT devices as an intrusion detection model. Still, compact and computationally minimal models are needed to be implemented in devices with restricted capabilities, such as IoT. Other development ideas for future work will involve probing more sophisticated pre-training techniques to investigate issues like unbalanced data or encrypted traffic. Adding detection, prevention and response measures into a portfolio of IoT security methodologies will complement IoT security. Large scale implementation will require the involvement of stakeholders of the industries in question. In conclusion, this study provides a practical and efficient way of detecting intrusion threats in real-time with low computational complexity to enhance the design of IoT security systems.

8 References

Adefemi Alimi, K.O. *et al.* (2022) 'Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things', *Journal of sensor and actuator networks*, 11(3), p. 32.

Alamro, H. *et al.* (2023) 'Modelling of Blockchain Assisted Intrusion Detection on IoT Healthcare System using Ant Lion Optimizer with Hybrid Deep Learning', *IEEE Access* [Preprint].

Alomiri, A., Mishra, S. and AlShehri, M. (2024) 'Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks', *International Journal of Computing and Digital Systems*, 16(1), pp. 645–659.

Alwahedi, F. *et al.* (2024) 'Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models', *Internet of Things and Cyber-Physical Systems* [Preprint].

Berger, S., Bürger, O. and Röglinger, M. (2020) 'Attacks on the Industrial Internet of Things–Development of a multi-layer Taxonomy', *Computers & Security*, 93, p. 101790.

Carter, R.E. *et al.* (2022) 'Model drift: when it can be a sign of success and when it can be an occult problem', *Intelligence-Based Medicine*, 6, p. 100058.

GHEZALA, C. and Radhwane, B. (2024) 'Time series data-based classification using combined 1D-CNN-GRU for Seizure detection and prediction'.

Hady, A.A. *et al.* (2020) ‘Intrusion detection system for healthcare systems using medical and network data: A comparison study’, *IEEE Access*, 8, pp. 106576–106584.

Iwendi, C. *et al.* (2021) ‘Security of things intrusion detection system for smart healthcare’, *Electronics*, 10(12), p. 1375.

Jeyanthi, D. and Indrani, B. (2023) ‘IoT-based intrusion detection system for healthcare using RNNBiLSTM deep learning strategy with custom features’, *Soft Computing*, 27(16), pp. 11915–11930.

Jullian, O. *et al.* (2023) ‘Deep-learning based detection for cyber-attacks in IoT networks: A distributed attack detection framework’, *Journal of Network and Systems Management*, 31(2), p. 33.

Khan, M.M. and Alkhathami, M. (2024) ‘Anomaly detection in IoT-based healthcare: machine learning for enhanced security’, *Scientific Reports*, 14(1), p. 5872.

Malik, F. (2022) ‘IoT Healthcare Security Dataset ICU Healthcare Security Dataset’. Available at: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset.

Merlino, V. and Allegra, D. (2024) ‘Energy-based approach for attack detection in IoT devices: A survey’, *Internet of Things*, p. 101306.

Qaddos, A. *et al.* (2024) ‘A novel intrusion detection framework for optimizing IoT security’, *Scientific Reports*, 14(1), p. 21789.

Ravi, V., Chaganti, R. and Alazab, M. (2022) ‘Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks’, *IEEE Internet of Things Magazine*, 5(2), pp. 24–29.

Sahu, A.K. *et al.* (2021) ‘Internet of Things attack detection using hybrid Deep Learning Model’, *Computer Communications*, 176, pp. 146–154.

Vailshery, L.S. (2023) ‘Statista. IoT connected devices worldwide 2019–2030-Statista’.
Verma, A. and Ranga, V. (2020) ‘Machine learning based intrusion detection systems for IoT applications’, *Wireless Personal Communications*, 111(4), pp. 2287–2310.

Xie, W. *et al.* (2022) ‘Evaluation of different bearing fault classifiers in utilizing CNN feature extraction ability’, *Sensors*, 22(9), p. 3314.