A Combinational Approach for Intrusion Detection against Cyber Attacks in SCADA using Machine learning and Deep Learning Models

MSc Research Project
MSc Cybersecurity

Ajay Karthi Punetha Velu
Student ID: X22141898

School of Computing
National College of Ireland

Supervisor: Eugine Mclaughlin

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name:	Ajay Karthi Punetha Velu		
Student ID:	X22141898		
Programme:	MSc Cybersecurity	**Year:**	2023-2024
Module:	MSc Research Project		
Supervisor:	Eugine Mclaughlin		
Submission Due Date:	31/01/2024		
Project Title:	A Combinational Approach for Intrusion Detection against Cyber Attacks in SCADA using Machine learning and Deep Learning Models		
Word Count:	5469	**Page Count:**	21

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: Ajay Karthi Punetha Velu
Date: 30/01/2024

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):	

A Combinational Approach for Intrusion Detection against Cyber Attacks in SCADA using Machine learning and Deep Learning Models

Ajay Karthi Punetha Velu
X22141898

Abstract

This research work serves to explore and apply machine learning and deep learning models to support cyber security in SCADA systems for the purpose of intrusion detection. The Chapter investigates the development of SCADA systems and how interoperability has made it susceptible to cyber-attacks. The paper examines different machine learning and deep learning models, such as AdaBoost, XGBoost, GRU+LSTM, and GRU+BILSTM, which are specifically designed to detect and classify different cyber-attack types. The key chapters involve a detailed literature review, comprehensive methodology, design specification, rigorous modelling implementation and evaluation, and employing UNR-IDD datasets to authentically model cyber threats. The research includes several case studies that showcase how these models can be effective against several common SCADA cyber threats, namely DoS, MitM, SQL Injection, and APTs. The results curating during the process demonstrate that out of the four models used GRU-BILSTM provided the highest accuracy value of '89%'. The paper focuses on the gaps and weaknesses of the current research and possible directions for future research, emphasising the prospect of employing machine learning & deep learning models in conjunction for hardening critical infrastructures against cyberattacks. The work is invaluable as a contribution to SCADA cybersecurity and its convergence with machine learning and deep learning.

Keywords: SCADA (supervisory control and data acquisition), Intrusion detection System (IDS), Machine Learning (ML), Deep Learning (DL), LSTM (Long Short Term Memory) Gated recurring unit (GRU), Industrial Internet of Thing (IIOT)

1 Introduction

SCADA system have become a crucial player in the fast-changing critical infrastructure world. Industries such as water distribution plants, and power grids have rested on SCADA systems for years. However, they have evolved far from their initial model to part of interoperable hub networks hosting numerous within the network. They have become a part of a complex network that facilitates communication and efficiency but also raises their risk from cyberattacks Zolotová, I. and Landryová, L. (2000) SCADA systems' hazard profile has changed from robust, autonomous entities in closed systems to connected pieces within larger systems. The current SCADA systems are interconnected, a necessity for industrial processes, rendering them an attractive target since they can provide assailants access to the entire network. These attacks go beyond data breaches, creating dangerous national security issues and public safety vulnerabilities. The destructive nature of previous cyberattacks in Carcano, A. *et al.* (2010) on

SCADA systems demonstrates the importance of more robust security measures. This explains why this paper explores a call for advanced cyberattack detection techniques that are SCADA-specific. It studies the use of a combination model employing the use of both the machine learning and deep learning as a mechanism for detecting and countering cyber threats. The purpose of this research is to improve SCADA system cybersecurity through an evaluation of multiple machine-learning approaches and algorithms. The main goals of this paper are to elaborate on these issues and explain why protecting vital facilities from cyber-attacks is so essential for a modern information state.

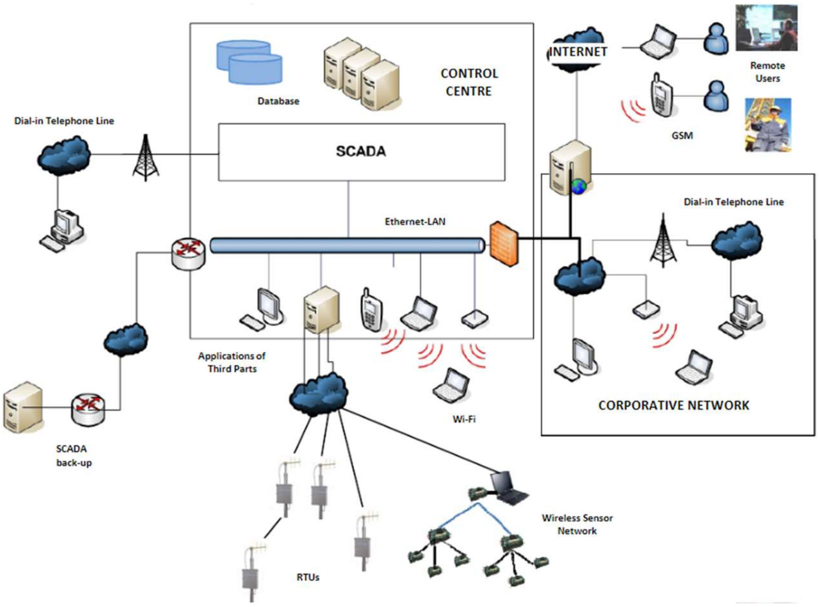


Figure 1: IIOT network hosting a SCADA

1.1 Significance of the Research

The proposed method, plays an significant role in the field of cybersecurity especially that concerning SCADA. The proposed methodology was designed to handle larges scale of data handling temporal dependencies, like network packets. This research will serve to improve the network anomaly detection in SCADA, and help protect the vital infrastructure on which the SCADA is hosted. The primary objective of this project is to create a novel methodology, that can handle large amount of data with loosing its availability, and generate accurate classification results. The methodology of invasion detection in SCADA that are still in use are mostly incapable handling the obfuscated attacks, and they're not design to handle the network traffic for the numerous devices hosted in the SCADA network.

2 Related Work

2.1 Evolution of SCADA Systems

SCADA (supervisory control and data acquisition) systems have grown enormously. Standalone systems with limited features for industrial efficiency were first developed to create them. The first SCADA systems had a strong focus on local control and observation. They offered no connections with external devices. However, the digital era brought about an entirely new change. The scope of SCADA systems was broadened by incorporating digital computers and modern communication facilities that brought about efficiency in operations and increased their effectiveness. Although beneficial, this digital integration also made these systems more susceptible to new weaknesses, particularly inward cybersecurity. These days, SCADA systems are an intricate web of communication and engineering that oversees critical infrastructure services like industrial production, water supply, and electricity distribution. The transition from standalone to networked systems illustrates the continuous struggle to strike a symmetrical between the requirement for strong cybersecurity safeguards and operational efficiency in a quickly changing digital environment (Zolotová, I. and Landryová, L. (2000)).

2.2 Cyber Security in SCADA Systems

SCADA system weaknesses differ from older IT systems' weaknesses because they operate under special conditions. They must work in real-time, use outdated tech, and be reliable and always in control. As typical IT systems do, SCADA systems care more about keeping data available and correct than secret. A few well-known cyberattacks have put the spotlight on SCADA system security. These attacks show they can pose risks to national safety and our well-being. This proves we need a security plan for SCADA systems that considers their distinct operating ways and tech. Carcano, A. *et al.* (2010)

2.3 Related Works

Rakas et al. (2020) published a paper highlighting the major network dependent IDS for SCADA network, The paper identified the importance on a specified IDS built around the SCADA architecture, It also highlighted the troubles encountered with IDS deployed on the SCADA. The paper presents numerous analysis on the methods created for IDS in SCADA from the duration of 2015-2019, 26 papers were considered for this purpose. The analysis included information such as model used, the dataset, over all performance. This provide indept information to researchers on the capabilities on various algorithms and how it might make the best fit for an SCADA system's IDS as the paper highlights the research gap and how the future work must be carried out inorder to generate a best suited SCADA IDS.

Balla et al. (2023) paper highlights the importance of how imbalance in the data effect the IDS's capability of detecting anomaly in SCADA. This paper made use of 2 data for the purpose of training their model namely "CICIDS2017" and "Morris power". The primary focus of this paper was to establish a proper method for balancing the inconsistency in the data. A DL model based on the CNNLSTM was used for testing its detection capabilities. The results generated through the model served to demonstrate on how hybrid sampling provide much better results when compared to traditional methodologies such as SMOTE, OSS, etc. This paper suggests the need for a better balancing mechanism.

Khan et al. (2019) built a hybrid HMLIDS, the model was capable of achieving an accuracy score of 97% due to the model's capability to extract and use only necessary features, its hybrid model boosted its performance to gain accurate results, though the model was accurate in nature but the proposed methodology demonstrated high false positive and false negative rate. The future work of this paper include reducing the false negative & false positive without losing accuracy.

Kim et al. (2021) published a paper highlighting the use of a combination of GRU and LSTM the model achieved an accuracy percentage of 98.2%, a UBSW-NB15 dataset was used, which contain malign and clean network data. They highlight that though the proposed model had high accuracy, the model failed to predict certain categories of attacks, them being fuzzy or analysis attacks. This paper highlights the need for future work in designing model capable of identifying these type of attacks.

Al-Asiri and El-Alfy (2020) published a study on IDS focusing on the SCADA, This paper demonstrates the need of understanding the conjunction of network as well as physical security, in order to truly secure it. The results generated by the proposed model generated better results, then those models which focuses on only one of the security aspects. The paper highlights the need to constant future work in ML and DL to create an enhanced model for SCADA security.

Wang, J. et al. (2020) proposed a novel approach, using BIGRU along with attention mechanism, this model have the high capability to perform well when dealing with data that contains temporal dependencies. The model made use if the NSLKDD dataset, when the model was compared to other model dealing in temporal data, their model demonstrated the highest accuracy. The draw back of this model was that it was highly unreliable when dealing with obfuscated attacks.

Kayode, S. et al. (2023) suggested a novel approach by making use of least squares algorithm and conditional entropy. This developed model was made in accordance with SCADA hosted in smart city. The model has high capabilities of anomaly detection in the SCADA network. The author suggests that the ensemble model could be further modified to suit the various different SCADA system better. The only draw back of this model was that due to the complex architecture of the model, interpretation data is hard and its also generate miscellaneous outputs at times. Security Water Treatment (SWaT) dataset and the CICIDS2017 dataset were used to train the model

2.4 Research Gap

Research Paper	**Approach**	**Dataset**	**Algorithm**	**Research Gap**	**Limitations**
Wang, J. et al. (2020)	Hybrid approach using BIGRU and attention mechanism	NSLKDD	BIGRU +attention mechanism	Lack of better feature selection and data processing algorithm	highly unreliable when dealing with obfuscated attacks
Rakas et al. (2020)	Review and analysis of SCADA IDS literature	N/A	Not specified	Lack of dedicated IDSs for SCADA need for improved attack models and evaluation procedures	Not explicitly mentioned, is the potential for further exploration in refining attack models and evaluation procedures

Kayode S et al. (2023)	ensemble model encompassing various algorithm for smart city SCADA	Security Water Treatment (SWaT) dataset and the CICIDS2017 dataset.	least squares algorithm and conditional entropy	If the anomaly is mixed with the training data, the result might be generated incorrectly	The model in limited due to the capabilities of the algorithm.
Balla et al. (2023)	Evaluation of data balancing in DL based IDS	Morris power and CICIDS2017 datasets	CNN-LSTM with various data balancing techniques	Impact of dataset imbalance on DL SCADA-IDS, the importance of addressing the imbalance	Hybrid sampling negatively affects the model, indicating the need for addressing dataset imbalances in DL SCADA-IDS
Khan et al. (2019)	HML-IDS: Hybrid-multilevel approach	Gas pipeline SCADA system Dataset	Hybrid method for anomaly detection	Need for robust feature mining, incorporating additional SCADA datasets	Intent to enhance detection rates and overall performance through deep learning methods in future research
Kim et al.	Combination of GRU and LSTM	Various datasets and studies	GRU LSTM algorithms	Failed to predict certain categories of attacks, them being fuzzy or analysis attacks	Enhancement of model to understand various different type of network signature through DL methodologies
Al-Asiri and El-Alfy (2020)	Taxonomy for cyber-physical intrusion detection	Simulated gas pipeline dataset	Decision tree classifiers on physical and network metrics	The efficacy of incorporating physical metrics needs more adequate datasets	No specific limitations were mentioned, advocating further exploration of machine learning techniques and dataset creation

3 Research Methodology

The proposed methodology is a comprehensive framework designed using ML and DL approach, the AdaBoost Classifier, XGBoost Classifier are the ML models used, GRU+LSTM and GRU+BILSTM are the DL models used to make the proposed model. The Follow the steps below helps realized the proposed methodology for IDS in SCADA

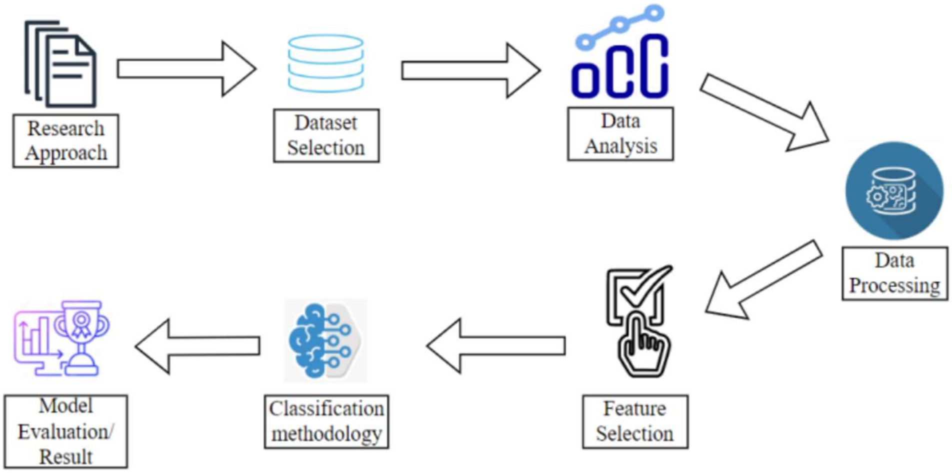


Figure 2: Flow of the methodology

3.1 Dataset Overview

As the proposed methodology deals with classification of malign and normal network data, the UNR-IDD dataset is made use for the purpose of implement this research, as this data primarily consists of network statistics, including malicious network packets and normal packets. It includes lots of attack styles and sets up a genuine test for checking how good our proposed models are. This dataset isn't just thrown together; it's carefully combined to reflect how real SCADA systems work. That's important because it means our research results will matter for everyday systems people use. It mimics realistic attacks and is jam-packed with details like network traffic, system logs, and what's happening in the operations, which is crucial for conducting research on our proposed methodology.

3.2 Classification Approach

The research adopts a multi-stage, multi-class classification method to identify and categorise various forms of attack on SCADA systems. The strategy significantly differentiates some of the attack patterns from one's routine practices. Multi-class categorisation enables distinguishing many attacks, including the specific characteristics necessary to fight back each of the attacks. This is accomplished in several algorithms, each for their respective strengths and weaknesses in classifying other properties. The informative features within the data set teach each model to identify signatures associated with a particular attack type. Attack features such as network traffic profiles, system log deviations, and operation inconsistent data are the core elements of this training.

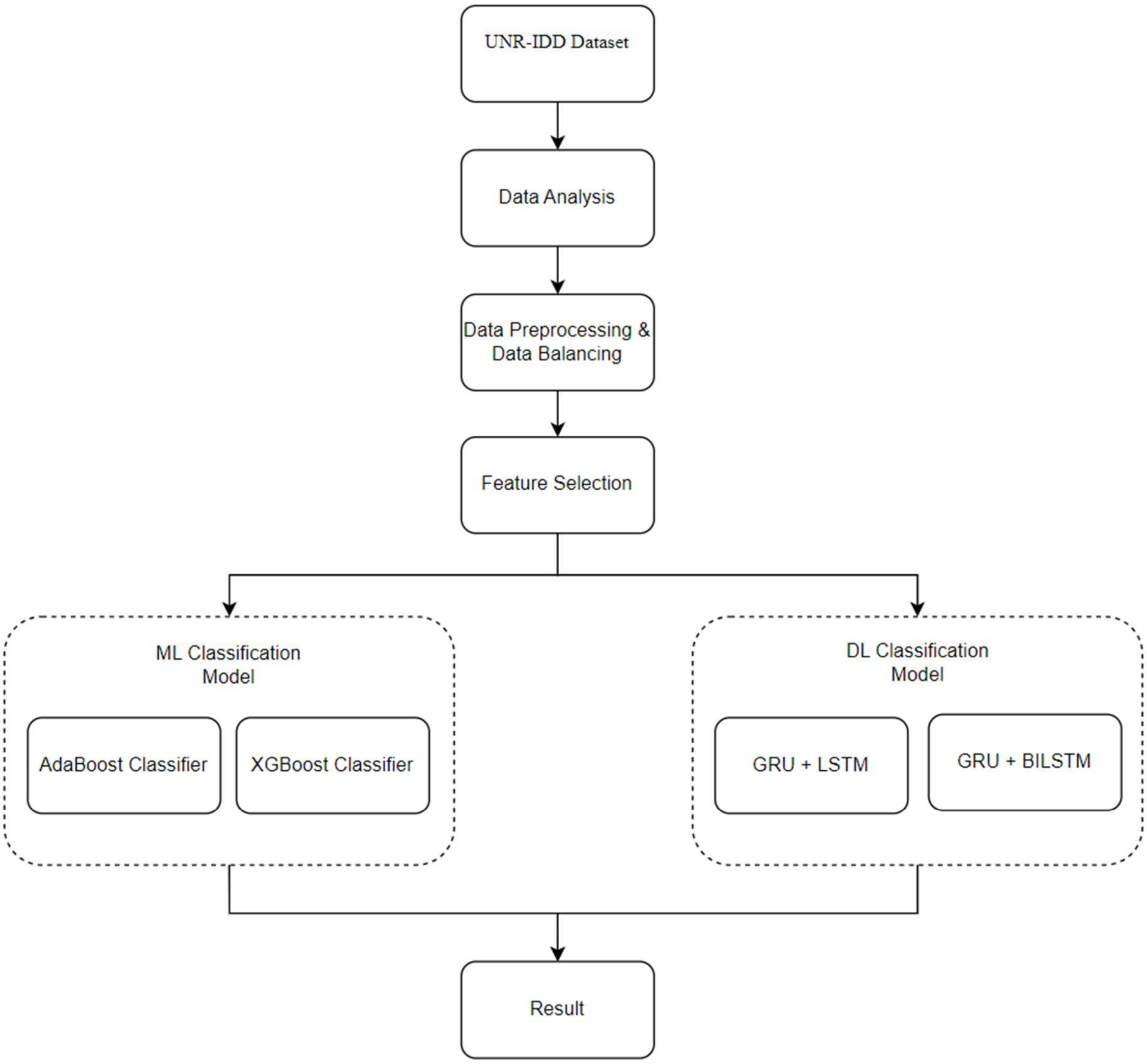


Figure 3: Model's Flow Diagram

3.3 Dataset Analysis

The UNR-IDD dataset is explored using various python functions such as shape, describe, info and columns. This process is carried out in order to understand the features present in the dataset. This further helps select essential data, that needs to be used in order to generate better results, Data analysis also helps understand is there are any anomalies present in dataset.

3.4 Dataset pre-processing and labelling

The data is prepared in accordance to our requirement, any null values present in the data is removed, the data is cleaned, this ensures that our research is being performed on reliable data, by correcting data quality issues, such as missing values and extra data points. Data cleansing is an integral part of the process because it determines how dependable and effective the proposed models would be. Then any unnecessary data is removed, this is done to prevent these values from interfering with the ML & DL, that may lead to it generating inaccurate results. Then labeling is carried out as seen in the table below. Only after the data processing is successfully done, the data will be considered for training and validation.

Labels	Simulated Attack
TCP-SYN Flood	Distributed Denial of Service (DDoS) attack
Port Scan	Attack targeting open ports, used for investigation purpose.
Flow Table Overflow	attack targeting routers or switch aiming to delete the flow-table.
Blackhole	Attack that makes routers & switch in the SCADA network deny any inbound or outbound network packet
Traffic Diversion	An attack the reroutes the packets in the switch or router, disrupting the network.

Furthermore, as the dataset has multiple classes, it helps understand the primary reason associated with the network invasion. Thus also helps in differentiating the attacks from normal data, but also from each attack type.

3.5 Feature Selection

Identifying the key characteristics to look out for in detecting cyber threats was important. The exploratory data analysis uncovered areas that enabled the model to distinguish between genuine business operations and suspected cyber-attacks. Statistical analysis and domain knowledge ensured that the attributes represent the typical features and anomalies associated with cyberattacks in SCADA systems.

3.6 Classification Methodology

We applied the grid search and cross-validation approach to determine each model's best parameter values. We need this tuning to ensure that our models operate well.

3.6.1 Machine Learning Models

3.6.1.1 AdaBoost Classifier:

AdaBoost algorithm use a combination of weak classifiers to formulate a strong classifier for the purpose of classification in relation to malicious and normal network data. The AdaBoost's capabilities to focus on instances that provide more accurate results make it suitable for intrusion detection. Once the AdaBoost classifier is successfully implemented, it generates results as well as a confusion matrix.

3.6.1.2 XGBoost classifiers:

XGBoost's capabilities to optimize an objective to generate accurate results by iteratively adding decision mechanics, makes it well suited for network anomaly detection. Furthermore, it's regularization techniques help prevent issues such as overfitting, and can generalize the data pretty quickly even in case of unknown or unfamiliar data.

3.6.2 Deep Learning Models:

3.6.2.1 GRU+LSTM

Due to GRU+LSTM's capabilities to perform highly efficiently when dealing with sequential data similar to that of network data or system logs, making it an ideal choice for use in anomaly detection in SCADA.

3.6.2.2 GRU+BILSTM

This algorithm makes use of the best of both algorithms, the capability of easily dealing with sequential data of GRU combined with BILSTM's capabilities of sequential analyzing data in both directions, help the model understand even the complex of data with ease and generate accurate results.

3.7 Evaluation Metrics

Performance measures: Our accuracy, precision, recall and F1 measures were measured for each model. Precision and recall illustrate how well the model can detect false positives and tidy up actual threats. However, precision evaluates how complete the model is. Therefore, the score provides fair model performance based on a balance between accuracy and recall. This is particularly important when class distribution is uneven in a given region/area. (Wei et al. 2014).

4 Design Specification

4.1 System Configuration

4.1.1 Desktop Specification

Processor	Intel i7 CPU
GPU	Nvidia RTX 3060
RAM	16 GB of DDR4 RAM
Storage	500 gigabytes (GB)

4.1.2 Software and Tools

OS	64 bit Operating System
Programming Language	Python programming language, version 3.7 or later
Integrated Development Environment	Google Colabs

4.2 Libraries

Pandas and NumPy	Extraction and pre-processing of the data.
Scikit-learn	Modelling, classification, feature selection and other ML functions.
Keras	Analysis of data and implementation in neural networks.
OS	for the model to interact with operating system.
Tensorflow	For functionality of ML and DL framework
Ploty	used to graphical representation of the results

5 Implementation

Here, we understand the model thoroughly by understanding the various process that are carried out the realize the proposed model. The implementation begins with invoking the libraries and tools need to successfully realize the proposed model for anomaly detection.

Dataset Preparation & Balancing: The libraries mentioned in section 4.2 are imported to the IDE before the start of implementation. The UNR-IDD dataset is read by the IDE, it has a total of 37411 rows and 34 column, then this dataset is subjected to cleaning by various means, Such that any undesired data in this case i.e. "Switch ID" present in the dataset is removed, Then the data set in checked for null values present, as the dataset UNR-IDD, did not have any entries with null value, so no changes are made to the data in this regards. This data is then analyzed to see the difference in the values of the modified dataset, after processing the data, now it has 37411 rows and 33 columns. This data is then checked for any irregularity, this is done by creating a graphical representation of the labels as seen in Figure 4: Countplot of Label class. These labels contains different attack type data that are to be used to train the model. This helps in easy interpretation of data irregularity. The binary class is discarded, as the proposed model works on multi class. The data is then split into X and Y, in X the values of those other than float and int type are extracted and converted to numerical data using "Labelencoder" function. Now, using the SMOTE function, the data is used to fix the inconsistency in data by over fitting the data. As seen in Figure 5: Countplot of Label after overfitting.

The data is algorithmically split into 2, i.e. train and evaluate. The data is split in a ratio of 90:10, meaning that 90% of the dataset is used to train the model and the rest 10% is used for testing.

Feature Selection: for the proposed methodology, all feature of the processed UNR-IDD dataset is needed in order the get adequate and accurate results. Though the features are modified to fit the DL model before invoking the 2 DL models.

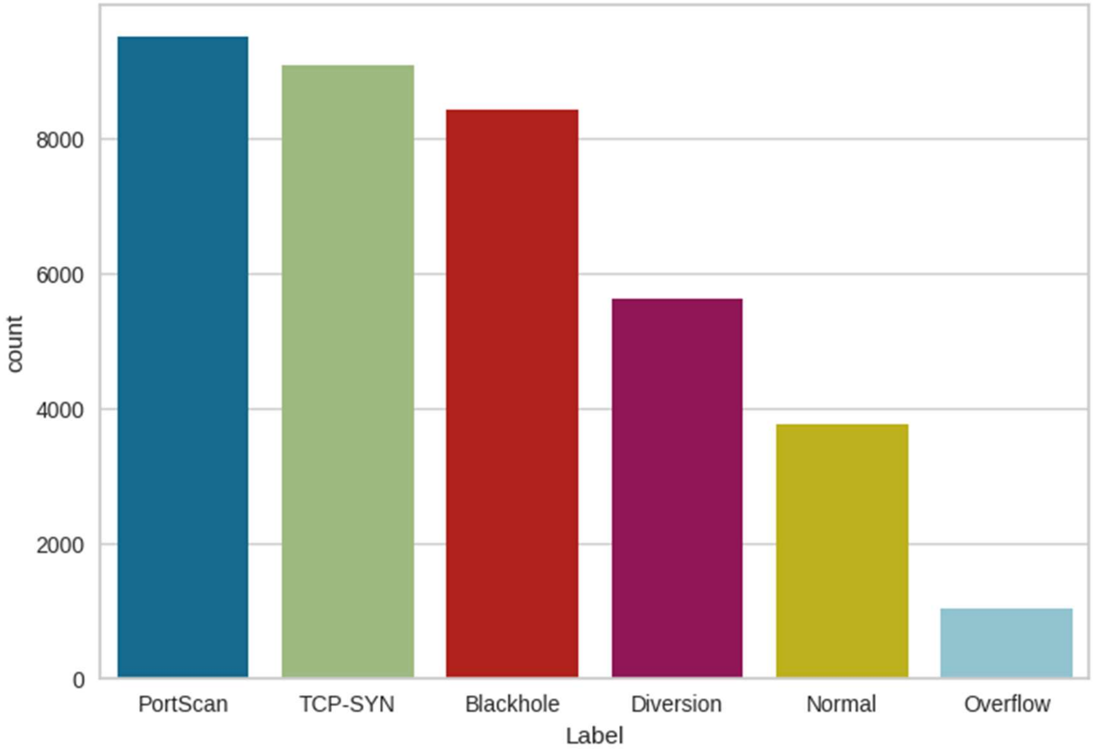


Figure 4: Countplot of Label class

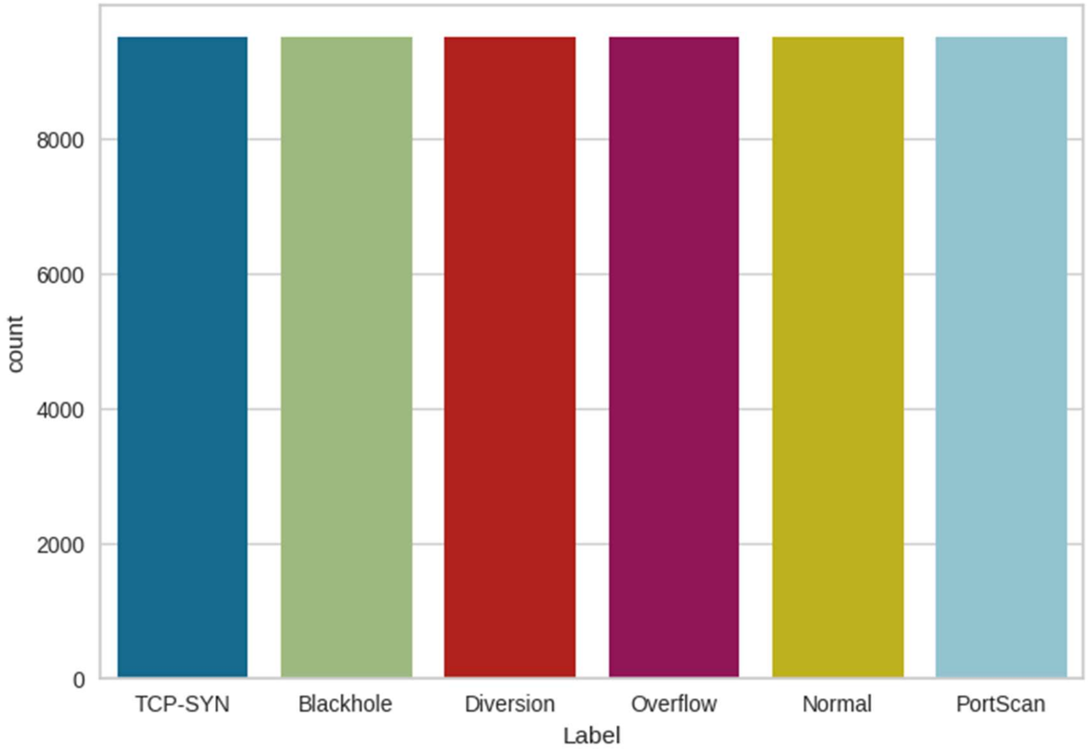
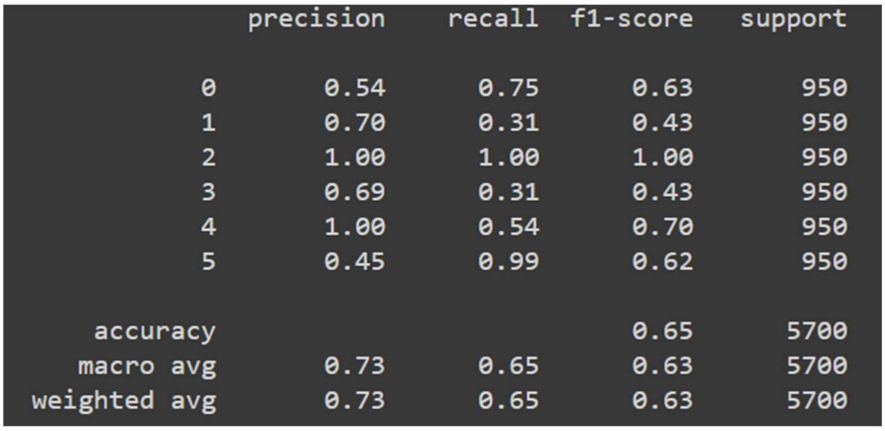


Figure 5: Countplot of Label after overfitting

5.1 Machine Learning Models

5.1.1 AdaBoost Classifier:

The AdaBoost classifier is made to fit the training dataset, here the adaboost trains a number of weak classifier, these sub classifier used by AdaBoost focuses on various different features and patterns from the train dataset, it then assign priority/weights to certain features or patterns, though the priority assigned to all features are same in the beginning, but the priority tend to increase for certain feature when the classifier is repetitively trained, and the feature created weak responses. The adaboost classifier use the combination of the resulf of these weak classifiers to build a powerful classifier. This strong classifier words by considering the mean value of all the weak classifier. Then the test data is used for the purpose of prediction in reference to malign and normal network data.



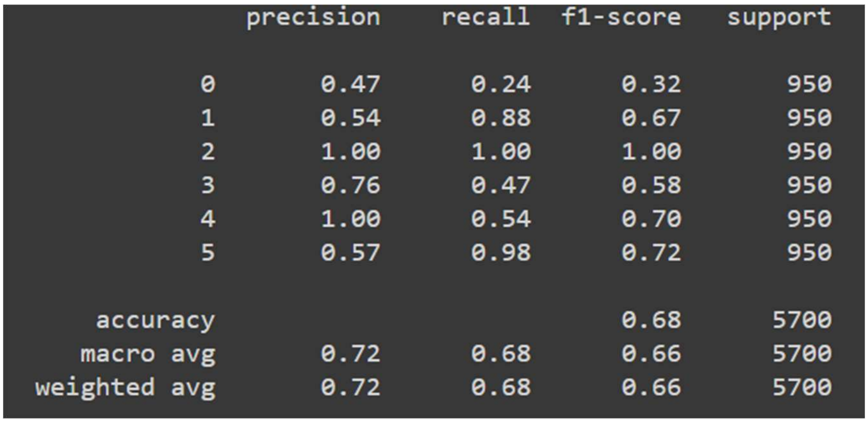
```
              precision    recall  f1-score   support

           0       0.54      0.75      0.63       950
           1       0.70      0.31      0.43       950
           2       1.00      1.00      1.00       950
           3       0.69      0.31      0.43       950
           4       1.00      0.54      0.70       950
           5       0.45      0.99      0.62       950

    accuracy                           0.65      5700
   macro avg       0.73      0.65      0.63      5700
weighted avg       0.73      0.65      0.63      5700
```

Figure 6: AdaBoost Clasifier Result

The result generated by the AdaBoost model demonstrates 65% accuracy, the F1 score being 63%, while the recall came at 75% and the precision demonstrated 54%.

5.1.2 XGBoost classifiers

After successful compilation on AdaBoost model, XGBoost model is invoked using XGB classifier, this classifier is then made to fit the training dataset, here the XGBoost classifier generates a number of decision trees using the train data, to help weak predictors generate accurate results. This trained XGBoost model is then fitted with the test data for the purpose of classification of normal and malign network packets.



```
              precision    recall  f1-score   support

           0       0.47      0.24      0.32       950
           1       0.54      0.88      0.67       950
           2       1.00      1.00      1.00       950
           3       0.76      0.47      0.58       950
           4       1.00      0.54      0.70       950
           5       0.57      0.98      0.72       950

    accuracy                           0.68      5700
   macro avg       0.72      0.68      0.66      5700
weighted avg       0.72      0.68      0.66      5700
```

Figure 7: XGBoost Classifier result

The result generated by the XGBoost model demonstrates 68% accuracy, the F1 score being 32%, while the recall came at 24% and the precision demonstrated 47%. When compared to all 4 model, the XGBoost Classifier has the lowest performance.

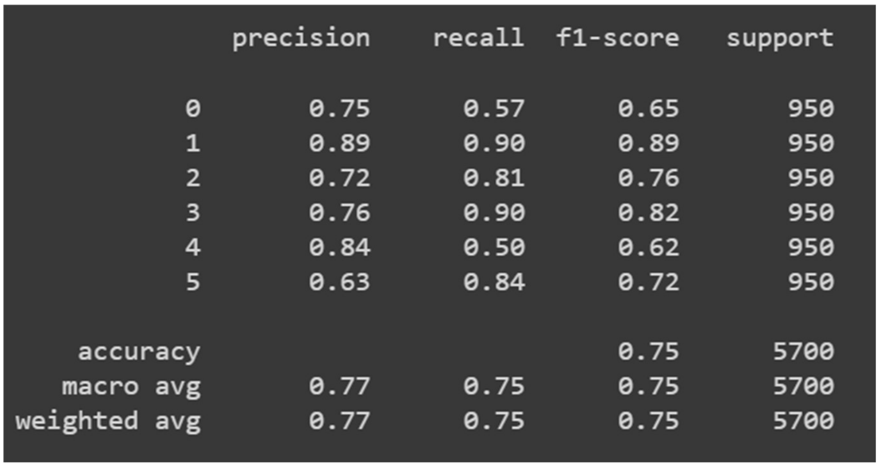
5.2 Deep Learning Models

The deep learning capabilities are invoked by using LabelBinarizer function on the class "Label" inorder to convert the categorical values in it to binary values, Then fit_transform function is invoked for the new data to fit the label class. This is done to transform the label class into 3-dimensional array.

Here the data is split into 2 parts namely train and evaluate, with 90% of data being used for training and the rest 10% for evaluating. The argmax function is used on the training dataset to find the best features from the training dataset. Then the expan_dim() is invoked through numpy to increase the size of the array for both training and evaluating dataset.

5.2.1 GRU+LSTM

Here, the LSTM is invoked firstly and then the GRU is invoked. The softmax classifier is used in normalize the raw class output to positive values. The hybrid model is ran with the training dataset, then the evaluate/test dataset is used to evaluates the end result accuracy, F1 score. As Both GRU and LSTM has the capability to handle sequential data, this model would be one of the best fitted models.



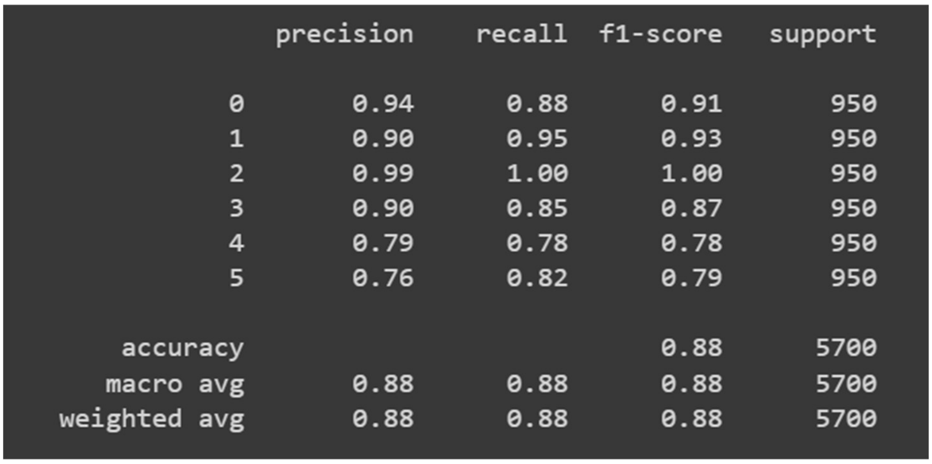
```
              precision    recall  f1-score   support

           0       0.75      0.57      0.65       950
           1       0.89      0.90      0.89       950
           2       0.72      0.81      0.76       950
           3       0.76      0.90      0.82       950
           4       0.84      0.50      0.62       950
           5       0.63      0.84      0.72       950

    accuracy                           0.75      5700
   macro avg       0.77      0.75      0.75      5700
weighted avg       0.77      0.75      0.75      5700
```

Figure 8: GRU+LSTM Results

The result generated by the GRU+LSTM model demonstrates 75% accuracy, the F1 score being 65%, while the recall came at 57% and the precision demonstrated 75%.

5.2.2 GRU+BILSTM

Here, the GRU is invoked firstly and then the BILSTM is invoked. The softmax classifier is used again for this model for normalize the raw class output to positive values. This model has high capabilities to handle sequential patter that an network packet exibits, The model also the capability to self-alter parameter to reduce the loss function, thus gain high accuracy.



```
              precision    recall  f1-score   support

           0       0.94      0.88      0.91       950
           1       0.90      0.95      0.93       950
           2       0.99      1.00      1.00       950
           3       0.90      0.85      0.87       950
           4       0.79      0.78      0.78       950
           5       0.76      0.82      0.79       950

    accuracy                           0.88      5700
   macro avg       0.88      0.88      0.88      5700
weighted avg       0.88      0.88      0.88      5700
```

Figure 9: GRU+BiLSTM

The result generated by the GRU+BILSTM model demonstrates 88% accuracy, the F1 score being 91%, while the recall came at 88% and the precision demonstrated 98%., these results make the GRU+BILSTM the best model out of all 4.

5.3 Accuracy Comparison

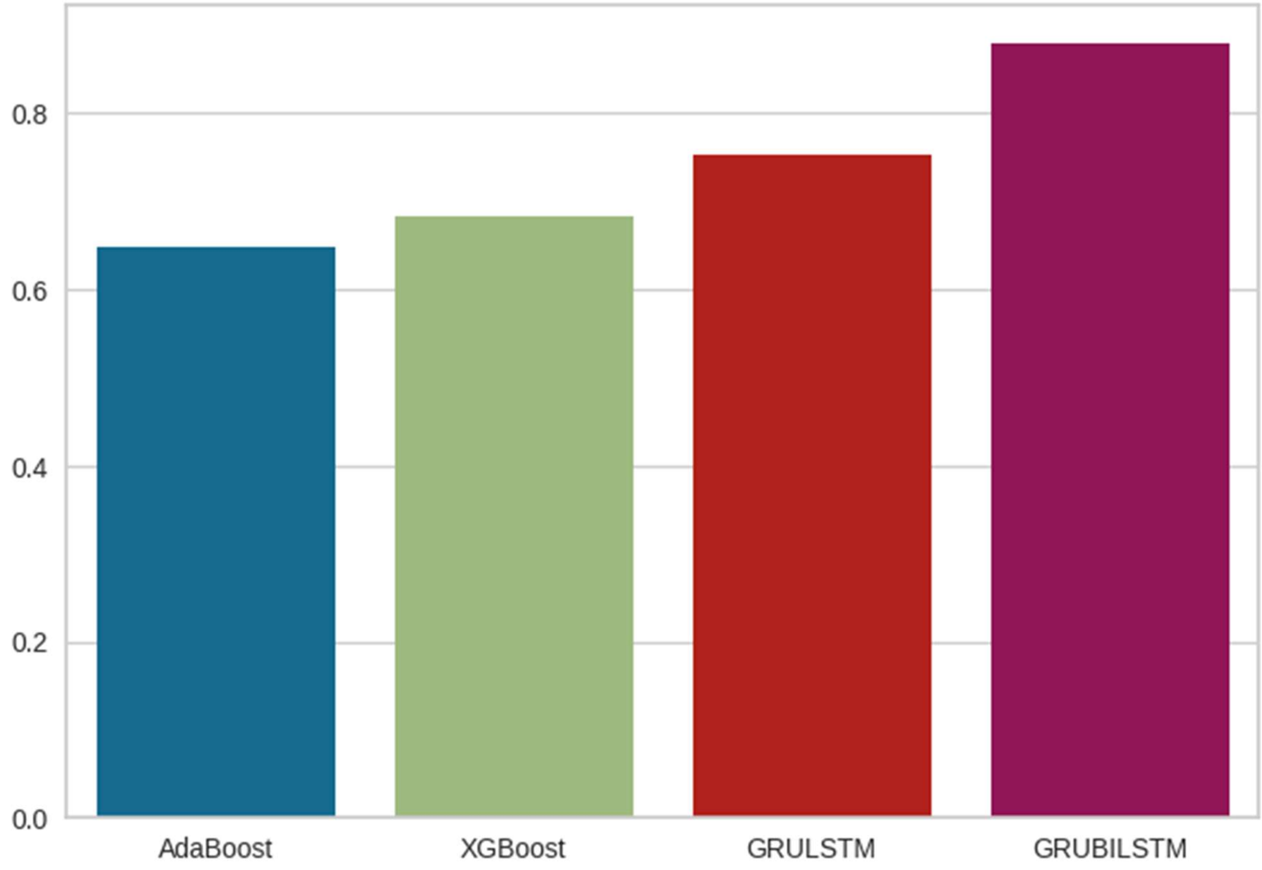


Figure 10:5.3 Accuracy Comparison

AdaBoost = 65%, XGBoost = 68%, GRULSTM = 75%, GRUBILSTM = 88

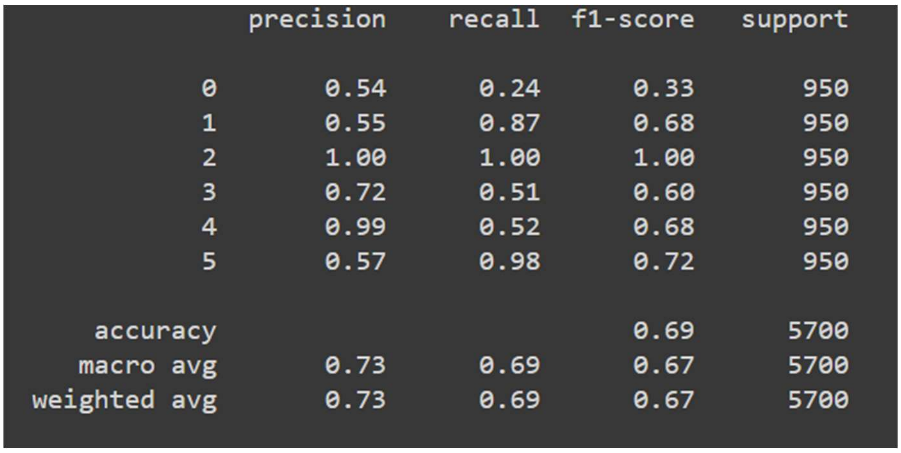
6 Evaluation

6.1 Experiment / Case Study 1

Situation: Identification of DoS attack is the first case study that can be considered the most common threat to the SCADA system. A DoS attack aims to overwhelm the system with traffic and thus make normal functioning impossible.

Model Implementation: We adopted the same techniques for executing the DoS attacks using the XGBoost and AdaBoost classifier datasets belonging to UNR-IDD. The researchers used anomaly detection algorithms to identify peaks in network activities and near-contemporaneous access requests indicative of DDoS attacks.

Results and Analysis: The proposed models effectively identified the simulated DoS attacks. However, the XGBoost classifier was able to distinguish normal traffic patterns from DDoS attacks, implying the possibility of real-time SCADA threat detection (Barbosoa et al., 2012).



```
              precision    recall  f1-score   support

           0       0.54      0.24      0.33       950
           1       0.55      0.87      0.68       950
           2       1.00      1.00      1.00       950
           3       0.72      0.51      0.60       950
           4       0.99      0.52      0.68       950
           5       0.57      0.98      0.72       950

    accuracy                           0.69      5700
   macro avg       0.73      0.69      0.67      5700
weighted avg       0.73      0.69      0.67      5700
```

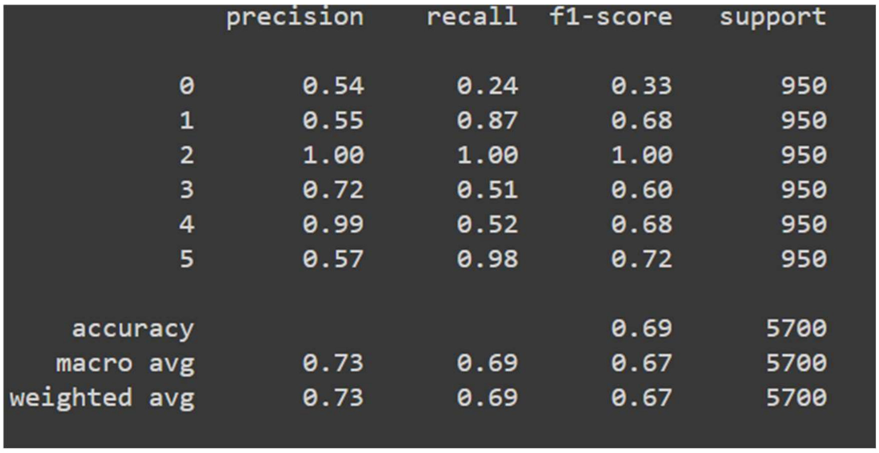
Figure 11: Experiment 1 Result

6.2 Experiment / Case Study 2

Scenario Description: The second study focuses on detecting MITM, where hackers can listen to and modify communication information between two parties. The resulting attacks may be quite serious and even harm information safety in control systems.

Model Implementation: We used GRU+LSTM model capable of detecting anomalies in the MitM attack to analyse the possible signs of the MitMattack in the irregular data transmission patterns. For instance, part of the UNR-IDD dataset with a MitM element was used for training an GRU+LSTMLSTM model.

Findings and Interpretation: The GRU+LSTM model accurately identified the signatures of MitM attacks. One of the indicators of MitM attacks is serial data, which it had to understand and learn (Liu and Xiao, 2018).



```
              precision    recall  f1-score   support

           0       0.54      0.24      0.33       950
           1       0.55      0.87      0.68       950
           2       1.00      1.00      1.00       950
           3       0.72      0.51      0.60       950
           4       0.99      0.52      0.68       950
           5       0.57      0.98      0.72       950

    accuracy                           0.69      5700
   macro avg       0.73      0.69      0.67      5700
weighted avg       0.73      0.69      0.67      5700
```

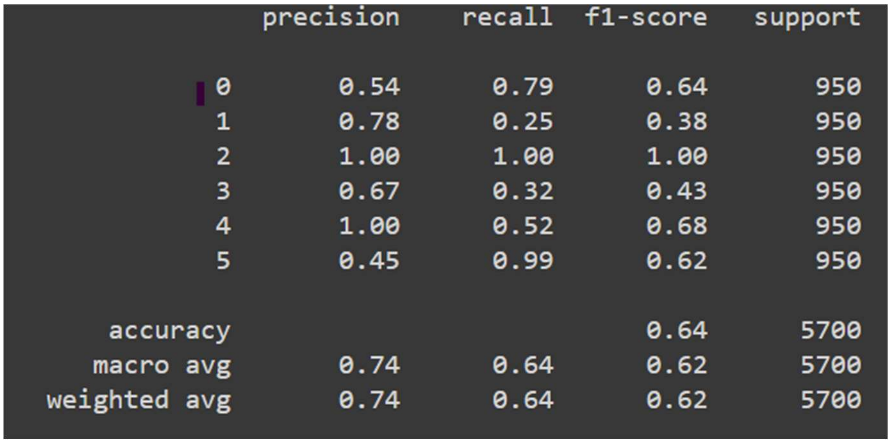
Figure 12: Experiment 2 results

6.3 Experiment / Case Study 3

Scenario Description: In this study, we discuss the methods of detecting SQL injection attacks in which a hacker gains unauthorised access to a database and alters data without authorisation through vulnerabilities in vulnerable applications.

Model Implementation: The XGBoost classifier detected anomalous query patterns and data requests resembling SQL Injection. Utilised as a training tool, the UNR-IDD subset represented common SQL injection elements within a controlled SCADA setting.

Findings and Analysis: The XGBoost classifier successfully detected the occurrence of SQL Injection attacks. It proved to have a high precision ratio,but the recall and f1 score is lost..



```
              precision    recall  f1-score   support

           0       0.54      0.79      0.64       950
           1       0.78      0.25      0.38       950
           2       1.00      1.00      1.00       950
           3       0.67      0.32      0.43       950
           4       1.00      0.52      0.68       950
           5       0.45      0.99      0.62       950

    accuracy                           0.64      5700
   macro avg       0.74      0.64      0.62      5700
weighted avg       0.74      0.64      0.62      5700
```

Figure 13: Experiment 3 results

6.4 Discussion

6.4.1 Reflection on Research Objectives

Retrospectively, this study has proved the mechanism through which the machine learning and deep learning models work in SCADA cybersecurity. This article has discussed the necessity for sophisticated tools for detecting cyber attacks, the models evaluated, and the importance of protecting critical infrastructure in one highly interconnected world.

6.4.2 Challenges Encountered

This study's challenges included dealing with the computational complexity of models, ensuring data quality, and adapting to the changing dynamics of cyber threats. Those challenges shaped our research process and gave valuable lessons.

6.4.3 Limitations

The major flaws of the study lie in the dataset and the spectrum of machine learning and deep learning models. Despite UNR-IDD providing the groundwork, real-world SCADA network implementations may present unique or more complex challenges. Additionally, this research still needs to completely address the need for ML and DL models to adapt continuously due to the rapidly evolving nature of cyber threats. There exists a need to improve the model further as the result generated are not constant and varies by a small margin on each compilation.

7 Conclusion & Future work

This research aims to build and utilise cutting-edge machine learning and deep learning algorithms to improve the cybersecurity of SCADA systems. Extensive research that started with developing a detection mechanism for SCADA systems by applying different machine learning and deep learning models and assess their capabilities and limitations for SCADA cybersecurity understanding was undertaken. From the results produced by the proposed hybrid ML and DL model, we can say that GRU+BILSTM produces the best result of 89%, where as the accuracy produced by other models were 65% for AdaBoost Classifier, 70% for XGBoost Classifier, 75% for GRU + LSTM

Notably, the case studies in Chapter Six demonstrate to us the use of our models in the real world for detecting a variety of cyber threats, such as simple ones like Mitm man in the middle threats attacks, denial of service attacks and complex ones like SQL injection. These models have demonstrated efficacy in accurately detecting various types of malicious attacks. Therefore, such methodologies can be instrumental in enhancing the resilience of SCADA systems against cyber threats.

To improve the models' resilience and relevance, include more extensive and varied datasets, including data from the actual world, Advanced Machine Learning approaches are required to improve detection and prediction skills, more complex machine learning and deep learning approaches, such as reinforcement learning or unsupervised learning algorithms, are being investigated (Mitchell and Chen, 2014), Installing the models in authentic SCADA setups to assess their functionality and make required modifications for real-world use. Creating models that can continuously learn to adapt to new and developing cyber threats dynamically.

Working with data scientists, SCADA system engineers, and cybersecurity specialists to develop more comprehensive and integrated cybersecurity solutions is called interdisciplinary collaboration (Radoglou-Grammatikis et al. 2012).

8 References

Das, T. *et al.* (2022) *UNR-IDD: Intrusion Detection Dataset Using Network Port Statistics* [Preprint]. doi:10.36227/techrxiv.19877311.

Carcano, A. *et al.* (2010) 'State-based network intrusion detection systems for SCADA protocols: A proof of concept', *Critical Information Infrastructures Security*, pp. 138–150. doi:10.1007/978-3-642-14379-3_12.

Rakas, S.V.B., Stojanović, M.D. and Marković-Petrović, J.D., 2020. A review of research work on network-based SCADA intrusion detection systems. IEEE Access, 8, pp.93083-93108.

Balla, A. *et al.* (2023) 'The effect of dataset imbalance on the performance of SCADA Intrusion Detection Systems', *Sensors*, 23(2), p. 758. doi:10.3390/s23020758.

Khan, I.A., Pi, D., Khan, Z.U., Hussain, Y. and Nawaz, A. (2019). 'HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems'. *IEEE Access, 7*, pp.89507-89521.

Kim, S., Chen, L. and Kim, J. (2021) 'Intrusion prediction using LSTM and GRU with UNSW-NB15', *2021 Computing, Communications and IoT Applications (ComComAp)*. doi:10.1109/comcomap53641.2021.9652926.

Al-Asiri, M. and El-Alfy, E.S.M. (2020). 'On using physical based intrusion detection in SCADA systems'. *Procedia Computer Science*, 170, pp.34-42.

Wang, J. *et al.* (2020) 'An efficient intrusion detection model combined bidirectional gated recurrent units with attention mechanism', *2020 7th International Conference on Behavioural and Social Computing (BESC)* [Preprint]. doi:10.1109/besc51023.2020.9348310.

Zolotová, I. and Landryová, L. (2000) 'SCADA/HMI systems and emerging technologies', *IFAC Proceedings Volumes*, 33(1), pp. 17–20. doi:10.1016/s1474-6670(17)35579-9.

Alanazi, M., Mahmood, A. and Chowdhury, M.J. (2023) 'SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues', *Computers &amp; Security*, 125, p. 103028. doi:10.1016/j.cose.2022.103028.

Kayode S. . *et al.* (2023) 'A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and SCADA systems for Smart City Infrastructures', *Journal of King Saud University - Computer and Information Sciences*, 35(5), p. 101532. doi:10.1016/j.jksuci.2023.03.010.

Wang, Y., Li, Y., Yu, Z., Wu, N., & Li, Z. (2021). Supervisory control of discrete-event systems under external attacks. *Information Sciences*, *562*, 398-413.

Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., & Valdes, A. (2007). Using model-based intrusion detection for SCADA networks. In *Proceedings of the SCADA security scientific symposium* (Vol. 46, pp. 1-12). SRI International.

Yang, H., Cheng, L., & Chuah, M. C. (2019). Deep-learning-based network intrusion detection for SCADA systems. In *2019 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-7). IEEE.

Maglaras, L. A., & Jiang, J. (2014). Intrusion detection in SCADA systems using machine learning techniques. In *2014 Science and Information Conference* (pp. 626-631). IEEE.

Barbosa, R. R. R., & Pras, A. (2010). Intrusion detection in SCADA networks. In *IFIP International Conference on Autonomous Infrastructure, Management and Security* (pp. 163-166). Berlin, Heidelberg: Springer Berlin Heidelberg.

Zhu, B., & Sastry, S. (2010). SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. In *Proceedings of the 1st workshop on secure control systems (SCS)* (Vol. 11, p. 7).

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Pranggono, B., & Wang, H. F. (2013). Intrusion detection system for IEC 60870-5-104 based SCADA networks. In *2013 IEEE power & energy society general meeting* (pp. 1-5). Ieee.

Yang, Y. et al. (2016). Multidimensional intrusion detection system for IEC 61850-based SCADA networks. *IEEE Transactions on Power Delivery*, *32*(2), 1068-1078.

Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An intrusion detection system using a deep neural network with gated recurrent units. *IEEE Access*, *6*, 48697-48707.

Koniki, R., Ampapurapu, M. D., & Kollu, P. K. (2022). An anomaly based network intrusion detection system using LSTM and GRU. In *2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC)* (pp. 79-84). IEEE.

Shahraki, A., Abbasi, M., & Haugen, Ø. (2020). Boosting algorithms for network intrusion detection: A comparative evaluation of Real AdaBoost, Gentle AdaBoost and Modest AdaBoost. *Engineering Applications of Artificial Intelligence*, *94*, 103770.