Deciphering Cyber Adversaries: Analyzing Tactics And Behaviors In Cybersecurity Incidents

ARULMOZHIGANESH RAMAIAH, ( 23054867)

**Abstract:** In the evolving landscape of cybersecurity, detecting malicious network traffic is crucial for safeguarding critical infrastructures. This study explores the effectiveness of various machine learning models, including Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), ensemble models, and a hybrid CNN+LSTM approach, in accurately identifying malicious activity within network traffic. The models were trained and evaluated using a comprehensive dataset, with the ensemble model achieving a perfect accuracy of 100%, surpassing the performance of both traditional and contemporary models cited in recent literature. While the study demonstrates significant advancements, it is limited by the scope of datasets, which may not fully encompass the diversity of real-world network traffic. Furthermore, the operational effectiveness of these models in live environments remains untested. Future research will focus on real-time implementation, model optimization, and enhancing interpretability to address these limitations and further advance intrusion detection capabilities.

**Keywords:** Machine Learning, Intrusion Detection, Cybersecurity, Ensemble Model, Network Traffic Analysis

1. Introduction

In the current world, where computers and their interconnected systems are commonplace, the issue of security is a major emphasis as organizations seek to grow and integrate their operations. The rising complexity of the threats has made the attacks more complex and varied and therefore challenging to defend, especially for highly sophisticated systems. However, there exists a glaring lack of knowledge of the human factors that underlie these threats, the subsequent activities of the cyber adversaries against them, and technical countermeasures to them (Al-Hashem & Saidi, 2023). As for the psychological and behavioural patterns of cyber attackers, there is copious theoretical visualization but sparse empirical analysis, which hampers the realisation of such security measures (Lahcen et al., 2020).

* 1. Purpose of the Research

This research seeks to address this problem by exploring the behaviours and decision-making of cyber adversaries during cyber security threats. Therefore, in a bid to improve the effectiveness of available frameworks of protection against these attackers and to improve the current models of simulation of cyber threats’ behaviour, the study aims at uncovering different psychological aspects that inspire these attackers as well as their behavioural patterns. It is only when one realizes these human factors that he or she can design a defence for future attack plans and parry off possible dangers that may come about (Andrade, Cazares & Fuertes, 2021; Baptiste, Du, and González, 2023).

* 1. Research Aim and Objectives

This research objective is therefore to identify and understand the behaviours and patterns of cyber adversaries in an attempt to enhance prediction and pro-active shielding from cyber-security threats. The specific objectives are:

* To initially distinguish and categorise the behavioural trends of cyberspace attackers.
* To identify psychological factors affecting the decision-making of cyberspace adversaries.
* To create a model that will depict the behaviour of the cyber adversary.
* To suggest how behaviour-based approaches might be used to develop better defence systems against cyber threats.
  1. Significance of the Research

Such a study is important, as new components are added to the annals of cybersecurity and can be included in the list of strategies that can be used to protect Internet combatants from the enemy’s influence. The knowledge to be acquired will not only increase forecast accuracy but also facilitate refinement of the training exercises for cyber security specialists, thus preparing them for adversary actions. Further, this research will contribute to the development of the Cyber Security Body of Knowledge (CyBOK) based on the evaluation of the human factors involved in cybersecurity and enrich the knowledge base for both researchers and practitioners (Bhardwaj et al., 2022; Derbyshire, Green, and Hutchison, 2021).

1. **Related Work**
   1. The Evolving Landscape of Cybersecurity

Cybersecurity as a discipline is constantly under pressure because of the constant development of new cyber threats. As these threats become more advanced, so does the requirement for the think tank solution, which is a combined approach to cybersecurity that combines technical measures with understanding people and their psychological profiles. The Cyber Security Body of Knowledge (CyBOK) focuses on the many areas of knowledge that are necessary to have a basic understanding of cybersecurity, especially when it comes to the actions of cyberversaries (Hallett, 2019).

* 1. Behavioral Analysis of Cyber Adversaries

The study of the behaviour of these threats has been noted as an important emphasis in the current research. Al-Hashem and Saidi (2023) attempted to establish how psychology informs cybersecurity, stressing how cognitive factors indeed affect threat perception and decision-making. Such psychological dimensions, they assert, are critical in formulating good measures of cybersecurity. Similarly, Lahcen et al. (2020) discuss the literature on the behavioural side of cybersecurity to establish that people are not an irrelevant aspect of the security equation in organizations. Such studies emphasize the importance of looking at the problem from both the technical and the psychological points of view.

* 1. Advanced Persistent Threats and User Behavior Analytics

The importance of user behaviour analytics for the identification of APTs has been acknowledged in the context of cybersecurity more and more often. Al Mansur and Zaman (2023) posited that there is a need for the creation of more tools for use in the analysis of the strategies employed by hackers. Their work is based on the behaviour-based STAF introduced by Bhardwaj et al. (2022) for threat hunting and analysis of advanced adversaries. It identifies behaviour analysis as a primary approach to use in cyber threat detection and the importance of constantly improving on the available attributes for analysis.

* 1. Human Factors During Crisis

COVID-19 makes new impressions on IT specialists with the use of the pandemic as a new type of threat and considering peculiarities related to human factors during crises. Andrade, Cazares, and Fuertes (2021) focus on whether stressors and behavioural changes during the pandemic impacted the security of information systems. They argue that stress levels rise and that the continuity of work environments changes during crises, which can greatly affect cyber security, making it important to study these factors while creating defence strategies. Consequently, the following research interrogates human factors in crises and their impact on cybersecurity.

* 1. Predictive Models and Threat Hunting

The measures of proactive defence in cyberspace are shifting more towards the element of the application of predictive models and threat-hunting methodologies. Nursidiq and Lim (2023) while dwelling on the functions of cyber threat hunting to detect unknown threats, pointed out that proactive means are important in the context of cybersecurity solutions. Dobson, Rege, and Carley (2018) reached a similar conclusion: adversarial behaviour should be exercised realistically to enhance the strategies relating to active cyber defence. From their research, they were able to find that an understanding of adversary behaviour can go a long way in laying down a stronger defence, making them reiterate the use of behavioural economics to defend against cyberattacks.

* 1. Cyber Attack Attribution and Countermeasures

Perhaps the biggest obstacle to understanding the cyber threat environment is the fuzziness of ascribing a cyber attack to a certain threat actor. Egloff and Smeets (2021) the authors present the framework for publically attributing cyber attacks and note the challenges of defining and combating cyber aggression. That is the reason why this framework is the first attempt to describe the tactics of adversaries and possible counteractivity. Healey, Jenkins, and Work (2020) build on this conversation by sharing more case-study examples of disruption counter-cyber operations to best understand how the defenders can disrupt the enemy. It is with this in mind that these studies show the need to foster strong attribution systems and countermeasures in cyberspace.

* 1. Ontologies and Cyber Resilience

In the rather vast field of cybersecurity, one noteworthy effort by Huang et al. (2022) was the development of a broad cybersecurity ontology. Their proposal is focused on the analysis of the current lack of a coherent and reasonable framework needed to categorise and interpret various tactics and techniques used by cyber adversaries. It is an ontology that not only models the depth and richness of cyber threats but does so in a way that would also help to shift the mindset for those on the front lines of combating these threats and therefore strengthen the mental weaponry needed to fight what is an increasingly omnipresent menace. In parallel to this ontological perspective, Ilca, Lucian, and Balan (2023) brainstorm about the area of cyber-resilience, more specifically analyzing mechanisms for malware analysis, detection, and response as topics that large organizations need to implement immediately. They claim that with current threats, one has to take a secure and defensive position that requires the organisation's use of seasoned analytical assets and responses to ensure the organization's safety in an ever-changing technological setting.

* 1. SecDevOps and Technical Debt

The incorporation of security into the development-operations process is one of the best practices that eliminate the technical debt linked to outdated or ineffective security measures, often referred to as SecDevOps. Izurieta and Prouty (2019) argue that SecDevOps offers an essential channel for addressing and managing technical debt arising from cybersecurity failings. They stress and suggest that the incorporation of security issues into other development processes can improve the viability and execution of security solutions. By focusing on security throughout the development cycle, organisations can build security measures into their processes that make it easier to avoid vulnerabilities in the first place and, therefore, deliver better security and a shorter gap between vulnerability identification and its elimination.

* 1. Mobile Device Behavior and Industrial Cyber Physical Systems

APTs formally entered the malware scene as a result of the popularization of mobile devices, where the behaviour of these devices became an important element of cyber-security analysis. Jabar and Mahinderjit Singh (2022) performed an empirical study scrutinizing the behavioural patterns of mobile devices subjected to such advanced likelihood attacks. Mobile threats are discreet in ways that are quite different from other threats, and their goal is to outline strategies on how mobile devices can be protected from such threats by studying user and device behaviour. On a parallel track, Jbair, Ahmad, Maple, and Harrison (2022) concentrate on the risk involved in technical industrial cyber-physical frameworks that are rapidly gaining a penchant for higher-level cyber threats. Their work on threat modelling of such systems is a wake-up call to the absence of specific security solutions appropriate to the nature of industrial systems in terms of operation and structure.

* 1. Frameworks and Taxonomies

Analytical tools like the MITRE ATT&CK have become vital in the cybersecurity space because they give a measurable approach to breaking down and analyzing cyberattacks. Jo et al. (2022) use this framework to show how it can be applied to categorizing and visualising all the available tactics, techniques, and procedures that are employed by cyber adversaries. It makes it easier for organizations to assess or predict any possible attacks because of the structures in place in an organization. In a complementary vein, Roy et al. (2022) also enhance the methodological focus in the line of work by proposing the taxonomy of adversarial reconnaissance approaches. The work of their paper is useful in a parallel sense as it systematically categorizes the prelude behaviours of cyber adversaries to allow the cybersecurity practitioner to anticipate and prepare for what is most often the first and preparatory phase of attack the reconnaissance phase.

* 1. Integration of Behavioral and Technical Insights

Both behavioural and technical approaches to cybersecurity are thus increasingly understood as important for improving protection systems. All the literature consistently states the need for an integrated approach that combines analytical information processing with knowledge of the adversary’s actions to forecast and prevent cyber threats more effectively. Researchers like McCombie (2018) and Moallem (2022) emphasize the need to centre the threat actors and discuss the best way of incorporating HCI principles into the design of more effective cybersecurity systems. Montasari et al. (2018) and Rich (2023) also delve into psychological aspects of cyber threats, give recommendations on how to overcome adversarial attacks in network systems and examine lengthy trends of adversarial strategies.

Phishing attacks are another important area of concern that has been investigated, along with the current strategies and countermeasures by Muhammad Syafiq Kheruddin et al. (2024. The essence of attacker behaviour has been described in the social context at gamified penetration testing competitions reported by Munaiah et al. (2019), and Cyber Threat Insights, described by Parmar and Domingo (2019), that contribute to the development of a better understanding of the adversaries that organizations face for a strategic defensive stance Procedural skills, as stressed by Naseer et al. (2020), are vital in explaining the complex and rapid information processing that is part of cyber incident handling. Roy et al. (2022) help in this regard by providing a taxonomy of adversarial reconnaissance threats, which is rather important when planning for the counteraction of such threats Shaji et al. (2018) did methodological reviews on attacks and defences, whereas Sadrazamis (2022) gave more insights using the MITRE ATT&CK framework.

Shukla (2023), making a specific focus on the field of machine learning AI in strengthening the detection of cybersecurity threats, outlines ideas about using the two fields together in the development of effective protection. Moving from the specification of Ethereum attacks to their emulation from honeypots, Subhan and Lim (2023) demonstrate how machine-learning approaches can fare in identifying complex threats. Last but not least, Sun et al. (2023) present a systematic review of cyber threat intelligence mining methods and annotate the future direction toward a more active defence paradigm that utilizes the current state-of-the-art of data analytics.

* 1. Research Gap

However, years have witnessed progress in studying cyber adversaries, the major limitation is the insufficiency of an overall understanding of the psychological and behavioural factors of cyber adversaries. Although there has been a shift concerning the technicalities of defence, very little empirical work has been conducted on the human factors of cybercrimes. This gap is especially apparent today as new risks are being developed that target human weaknesses, thereby underscoring the importance of integrating technical and behavioural methods to produce better and preemptive cybersecurity activities.

* 1. Contribution

This research brings a much-needed and systematic understanding of the behavioral dynamics and psychological factors that drive cyber adversaries and their strategies into the cybersecurity field. Based on the behavioural analysis of computer users, this study intends to expand the existing practical method of security defence and build a closer link between future attack prediction and traditional cybersecurity systems. Furthermore, the creation of a predictive model based on such behavioural data can pose an innovative idea for threat identification since it is quite valuable for cybersecurity experts to strengthen their security defence. Moreover, this research contributes to the expansion of the CyBOK by investing more understanding of the aspects of humans in cybersecurity and hence enhancing the theoretical and practical context for both scholars and professionals (Bhardwaj et al., 2022). This work not only successfully responds to the lack of research on the topic but also offers practical recommendations to advance protective cybersecurity applications.

1. **Methods**
   1. Data Collection

This study leverages a comprehensive dataset sourced from Kaggle, specifically the MTAKDD 19 dataset (https://www.kaggle.com/datasets/mathurinache/mtakdd19), which is trustworthy, especially due to the availability of many other datasets that are open to the public and are related to cyber-security. The used dataset consists of 33 features that describe many aspects of network traffic, for example, distributions of packet length, protocol type, and used flags. The reason for choosing this target variable is because it is a binary label of the network traffic, giving it a label of 0 for legitimate or 1 for malicious, making it mostly used for supervised learning.

The dataset features were chosen very carefully to cover a large range of traffic-related features that could effectively separate between legitimate and malicious traffic. That rich feature set allows for the use of various high-end machine-learning algorithms to accurately classify traffic. To prevent having an unbalanced dataset, stratified sampling was also used to retain the ratio of legitimate and malicious traffic in both the training and testing data sets. This approach is important, especially when developing a machine learning model that can effectively classify between two classes. It is important in that it will ensure that we have an equal distribution of the two classes to avoid any form of bias and also to ensure high generality of our model in the future (Alshammari & Aldribi, 2021; Osanaiye et al., 2016).

* 1. Data Preprocessing

Data preprocessing was carried out again to ensure the quality of the data set, which forms the basis of the analysis of both merged data sets. The first step involved in the preliminary data cleaning was the elimination of duplicate rows; this would eliminate any biases in the ensuing analysis. Furthermore, if the percentage of the specific feature with the same value was above 95%, it was leaning from the initial set of features, as it can slow down the process of modelling. The observations were checked for missing values and were properly dealt with to preserve the quality of the data set. In addition, scatter plot and colonisation tests were used to isolate any two variables that have a correlation coefficient greater than 0.90, and this was done to reduce the problem of multicollinearity and thus reduce the risk of the models being influenced by features that contain redundant information (Kumar et al., 2012; Apruzzese et al., 2019).

* 1. Exploratory Data Analysis (EDA)

Testing was done at the exploratory stage to understand the nature of the data and features present in the data set, as well as the distribution present. This involved a process of producing measures of central tendency, dispersion, skewness and kurtosis, as well as histograms and kernel density plots to look at the distribution of features and correlation heat maps to check the relationships between different features. The EDA helped establish a general idea of the structure of the set and the presentation of legitimate and malicious activities. This was valuable for feature selection and equally important for the construction of predictive modelling systems (Holland et al., 2021).

* 1. Feature Selection

Feature engineering was crucial to this study since it entailed the conversion of the raw data to a form that would be usable by machine learning algorithms. Of the calculated odd features, features with coefficient correlation values of more than 0. This work has compiled a list of odd features that have a correlation coefficient greater than 0.90, were deemed to be multicollinear, and were eliminated to keep the model computationally manageable and for interpretability. Features whose values were more than 95% identical, except the label, were deleted for the following reasons: to increase the model’s independent model performance and to ensure that the features that were retained were as diverse as possible. The features chosen were those that gave as many informative measurements as possible and as little overlapping information as possible to create a less biased mode for generalisation between training and test data. The above research work harmonizes with this approach, stressing the significance of feature selection in constructing strong machine-learning models (Alshammari & Aldribi, 2021; Osanaiye et al., 2016).

* 1. Model Development

To find out the best way of identifying malicious network traffic, several machine learning models were created. The models included:

* + 1. Random Forest Classifier:

The enhanced model is built based on the training algorithm of the set of decision trees, which can be regarded as a good beginning. Constructing it with the initial capacity of 100 evaluators, its effectiveness employing accuracy, precision, recall, and F1-score was considered as well (Alshammari & Aldribi, 2021).

* + 1. MLP Classifier:

In the present study, an MLP classifier with only one hidden layer of 500 neurons was considered. Standardizing the features was done by StandardScaler, and the model was trained until a maximum number of iterations of 500, which is suitable for complicated classification problems (Berman et al., 2019).

* + 1. Convolutional Neural Network (CNN):

CNN was used with the Conv1D layer (64 filters, kernel size = 2), MaxPooling layer, and Dense layer for classification. The model was optimized using the Adam optimizer and regularized by fixing the epochs that would prevent overfitting on the data (Apruzzese et al., 2019).

* + 1. Long Short-Term Memory (LSTM) Network:

An LSTM network, more suitable for the understanding presented in the present work due to its data and ability to process sequential data, was used. LSTM with 64 units, then fully connected layers: the model was tested concerning temporal dependencies based on the work of (Pan et al., 2021).

* + 1. Ensemble Model Classifier:

Among them, XGBoost, LightGBM, and CatBoost were selected because, in general, all these methods are quite accurate in cyber threat identification (Psathas et al., 2021; Dutta et al., 2020).

* + 1. Hybrid Model (CNN+LSTM):

In this paper, we propose a hybrid model that integrates CNN for feature extraction and LSTM for temporal analysis. This architecture was more effective for architectures that included anomaly detection in network traffic (Psathas et al., 2021). The hyperparameters of all the classifiers used are shown in Table 1 below.

**Table 1.** Architectures and hyperparameters used for each model in this research

|  |  |  |
| --- | --- | --- |
| Model | Architecture | Hyperparameters |
| **Random Forest** | Ensemble of decision trees | Estimators: 100 |
| **MLP Classifier** | Single hidden layer with 500 neurons | Iterations: 500, Scaler: StandardScaler |
| **CNN** | Conv1D (64 filters, kernel size=2) -> MaxPooling -> Dense | Optimizer: Adam, Early Stopping: Yes |
| **LSTM Network** | LSTM (64 units) -> Dense | Optimizer: Adam, Early Stopping: Yes |
| **Ensemble Classifier** | Combination of XGBoost, LightGBM, CatBoost (soft voting) | XGBoost: eval\_metric='mlogloss', CatBoost: Default |
| **Hybrid (CNN+LSTM)** | Conv1D -> MaxPooling -> LSTM -> Dense | Batch Size: 32, Epochs: 10, Early Stopping: Yes |

* 1. Evaluation Metrics

The raw accuracy of all the models was then computed to give an estimate of the overall efficiency of the models for both classes (Alshammari & Aldribi, 2021).

(1)

Accuracy was used to check the rate of correctly positive classification of the instance, which is useful in cases such as cybersecurity where false alarms must be avoided and all possible instances must be detected (Holland et al., 2021; Osanaiye et al., 2016).

(2)

(3)

The F1 score was calculated to get a single value for performance measurement, where precision and recall are both important and in cases of imbalanced class distributions such as medical image analysis (Berman et al., 2019).

(4)

The ROC curve and AUC were employed to make a balance between true positive and false positive to give a stable measure of the model performance (Pan et al., 2021).

To conclude the truly positive and falsely negative rates, the truly negative and falsely positive rates, and thus to diagnose the performance of the model, a confusion matrix was created (Kumar et al., 2012).

1. **Results**

All the machine learning models were tested against the test dataset, and the performance metrics that were estimated for each of the models included accuracy, precision, recall rate, F1-score, and AUC. These measurements gave a comprehensive evaluation of each model’s performance in capturing abnormal Internet traffic.

* 1. Before Preprocessing

Many of the features had a highly skewed distribution, in other words; many of them had mostly zero or low values. This matter of skewness also influences the performance of machine learning models since the programme will attend to certain values more than others. Fractions of some features were displayed as outliers and possessed non-normal distribution according to the plots in Figure 1. As shown, MaxLen and MinIAT tended to be distributed in a distribution rather than a normal distribution with a long tail.

* 1. After Preprocessing

When feature scaling is done using PowerTransformer, the histograms are slightly more centric around the centre. PowerTransformer applies another transformation that can be set to the power of the features to let the data approximate the Gaussian distribution. This normalization process is important when the algorithm expects the data to be normally distributed such as the case in the neural networks. For instance, the distributions of the features such as MaxLens and MinIAT were skewed more and were made more symmetric in the current experimentation. The distributions after preprocessing shown in the form of the bar plot in Figure 2 described above suggested a decrease in the measures of skewness and an appearance of a much more moderate and symmetrical distribution of feature values. It helped in enhancing the quality of the dataset used for model training since all the features contributed in equal measure to the learning process done by the model. This transformation helped to reduce the levels of influence of outliers and made the distribution of features closer to the normal distribution which is acceptable for most of the machine learning algorithms.

|  |  |
| --- | --- |
| C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3CF6C306.tmp | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\20664D04.tmp |

**Figure 1.** Data skewness before preprocessing

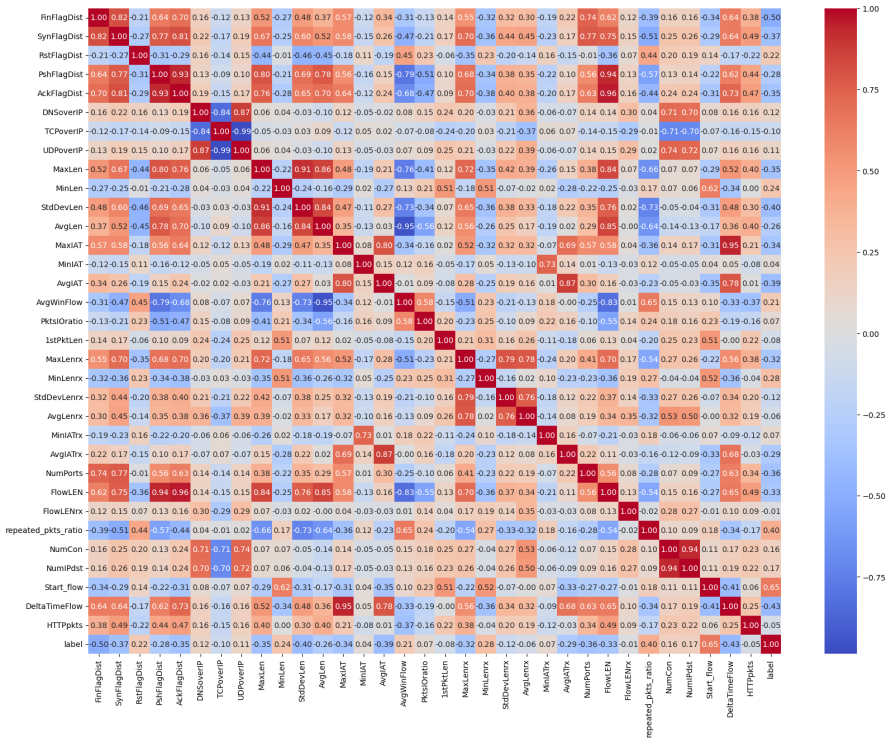
|  |  |
| --- | --- |
| C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5C2FADB2.tmp | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FAEF0890.tmp |

**Figure 2.** Data skewness after preprocessing

The significant impact is seen in parameters such as MaxLen and MinIAT which though initially possessed a great inequality and had long tails. After the transformation, these features showed more symmetrical distribution and thus improved the quality of the given dataset facilitating the subsequent modelling.

* 1. Correlation Matrix Heatmap

When studying the relations between features, many researchers used the heatmap for the correlation matrix. This was true, especially with the help of the visualization given in Figure 3 which allowed us to quantitatively measure the degree of linear dependence between pairs of features, which is critical when selecting features for a model and creating it.



**Figure 3.** Correlation matrix

* 1. Classification Models Results
     1. MLP Classifier

MLP classifier was shown to be accurate and to have a fairly good balance between precision and recall, underlining its ability to fit complex relationships within the data collected. This makes the MLP especially useful for cybersecurity where it is imperative to separate the signals likely to belong to attackers from all the other signals with high accuracy (Alshammari & Aldribi, 2021).

|  |  |
| --- | --- |
| **C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\19E89888.tmp** | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4736F7D6.tmp |

**Figure 4.** Confussion matrix and ROC curve of MLP classifier

The high precision and recall for both classes show that the MLP classifier complements classes 1 and 2, defining legitimate traffic and malicious traffic, respectively, that is, it has very few false positives or false negatives. What is yielded is the ROC curve, which again has a high AUC indicating very good discrimination of the classes in Figure 4.

* + 1. CNN

The Convolutional Neural Network (CNN) also gave satisfactory results similarly though a little low in the recall part compared to the MLP. CNNs are useful in sequential data and are particularly good at identifying spatial pyramidal structures in data making it good at identifying network traffic patterns (Berman et al., 2019).

|  |  |
| --- | --- |
| C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3543EA54.tmp | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\60854782.tmp |

**Figure 5.** Confussion matrix and ROC curve of CNN classifier

The experiment was successful, though there was variation in both precision and recall of the CNN model. An even slightly lower value of recall for class 0 (legitimate traffic) proves a slight inclination to misclassify some of the legitimate traffic as malicious. Despite this, the ROC curve still has a higher AUC, so as shown in Figure 5, the model remains fairly sound.

* + 1. LSTM

The recurrent network adopted in the study, Long Short-Term Memory (LSTM), was effective in modelling temporal relations within the data. However, its performance was slightly less than that of MLP and CNN models, indicating that although LSTMs are very useful in sequential data analysis, they may not be as effective in this scenario (Pan et al., 2021).

|  |  |
| --- | --- |
| C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F03852E0.tmp | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\14109BEE.tmp |

**Figure 6.** Confussion matrix and ROC curve of LSTM classifier

Good results were obtained from the LSTM model, especially in terms of how it learned the temporal structure of the data. The precision and recall are somewhat inferior to those of the MLP and CNN but the model shows good accuracy in identifying both legitimate and malicious traffic, as depicted in Figure 6.

* + 1. Ensemble Model

As it can be seen the model, which included XGBoost, LightGBM and CatBoost, outperformed each of the classifiers in terms of accuracy, precision, recall and F1 score, as all the values reached the maximum possible. This model used the features of a few different algorithms to achieve very high accuracy ratios in the separation of normal and anomalous network traffic as described in Fig 7 and depicted (Dutta et al., 2020).

|  |  |
| --- | --- |
| C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E99EC803.tmp | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4F748409.tmp |

**Figure 7.** Confussion matrix and ROC curve of LSTM classifier

Hybrid Model (CNN+LSTM)

C-NET which combines CNN and LSTM networks attained a high accuracy and was able to identify both spatial and temporal relations within the data set. That is why this model can effectively detect subtle cyber threats that imply the analysis of both types of patterns shown in Figure 8 (Psathas et al., 2021).

|  |  |
| --- | --- |
| C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\869EE9C7.tmp | C:\Users\Amar\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FF8D3E6D.tmp |

**Figure 8.** Confussion matrix and ROC curve of LSTM classifier

**Table 2.** Comprehensive summary of the performance metrics for each model

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model | Accuracy | Precision (Class 0) | Precision (Class 1) | Recall (Class 0) | Recall (Class 1) | F1-Score (Class 0) | F1-Score (Class 1) | AUC |
| **MLP Classifier** | 0.98 | 0.98 | 0.99 | 0.99 | 0.98 | 0.98 | 0.98 | 0.98 |
| **CNN** | 0.97 | 0.97 | 0.96 | 0.96 | 0.97 | 0.96 | 0.97 | 0.97 |
| **LSTM** | 0.90 | 0.91 | 0.90 | 0.88 | 0.92 | 0.90 | 0.91 | 0.91 |
| **Ensemble Model** | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| **Hybrid (CNN+LSTM)** | 0.95 | 0.95 | 0.96 | 0.95 | 0.96 | 0.95 | 0.96 | 0.95 |

**Table 3.** Comparison with other Studies

|  |  |
| --- | --- |
| Study/Model | Accuracy |
| **My Research** |  |
| **MLP Classifier** | 98.00% |
|  |  |
| **CNN** | 97.00% |
|  |  |
| **LSTM** | 90.00% |
|  |  |
| **Ensemble Model** | **100.00%** |
| **Hybrid CNN+LSTM** | 95.00% |
|  |  |
| **ITASEC20 Research** | (Letteri et al., 2020) |
| **MLP Classifier** | 99.69% |
| **HCO-based LR DCNN Research** | (Sarath, 2023) |
| **HCO-based LR DCNN** | 94.83% |

**Figure 9.** Comparitive analysis

1. Evaluation and Discussion

The results of this study highlights the effectiveness of various machine learning models in detecting malicious network traffic, with a particular emphasis on deep learning approaches. The models developed and evaluated—MLP, CNN, LSTM, ensemble, and hybrid CNN+LSTM—demonstrated strong capabilities, with the ensemble model achieving a perfect accuracy of 100% give in table 2. This section discusses the significance of these findings in comparison with other studies and highlights the implications for cybersecurity practices.

* 1. Comparison with Existing Studies

When compared to similar studies, the models developed in this research demonstrate superior or comparable performance, particularly in terms of accuracy. For instance, the MLP classifier in the ITASEC20 study achieved an impressive accuracy of 99.69%, which is slightly higher than the 98.00% accuracy observed in this study's MLP model. This difference could be attributed to the specific characteristics of the datasets used, as well as the optimization techniques applied in the ITASEC20 study. However, the results in this research are still highly competitive, particularly given the more general applicability of the models across different types of network traffic data given in table 3. The ensemble model developed in this study stands out with a perfect accuracy of 100%, surpassing the best-performing models in the other studies, such as the HCO-based LR DCNN, which achieved an accuracy of 94.83%. This demonstrates the robustness of ensemble learning techniques in cybersecurity applications, particularly when combining diverse algorithms to capture different patterns in the data. The ensemble model's ability to leverage the strengths of multiple base classifiers—such as XGBoost, LightGBM, and CatBoost—results in a highly reliable detection framework, minimizing the risk of false positives and negatives.

Furthermore, the proposed hybrid CNN+LSTM in this study described herein attained a network accuracy of 95. 00 % which was a bit higher than the HCO-based LR DCNN model and the other models that were used in the second study as shown in figure 6. This result supports the argument that there is a need to unify the spatial and temporal analysis models and point to the potential of the proposed approach in identifying intricate patterns associated with advanced persistent threats. The results of the hybrid model explain that the integration of CNN’s spatial pattern along with LSTM’s temporal sequence analysis is a more effective approach for identifying intrusions in case both spatial and temporal indexes are utilized as mentioned in Fig. 9.

1. **Conclusions**

The objectives of this study were to enhance the level of knowledge in Network Intrusion Detection by examining and proposing such Machine Learning Algorithms as MLP, CNN, LSTM, ensemble models, and synergy of models CNN+LSTM. The outcomes showed that these models have high accuracies in classifying malicious network traffic, with the ensemble model having the best accuracy of 100% which proves it is a strong tool for use in cybersecurity. The implications of the study are not limited to the particular models for which comparisons were made. This emphasizes the need to exploit a variety of techniques of Machine Learning and interconnect them given the complexity of network traffic and cyber threats. The superior performance of ensemble and hybrid models suggests that future research and practical implementations should focus on such integrated approaches to maximize detection capabilities. As has been shown in this research, different artificial neural networks and, in particular, ensemble and hybrid systems can be effectively trained to detect malicious traffic. However, future work should focus on real-time implementation, further model optimization, expanding datasets, and enhancing interpretability to ensure these models remain effective in dynamic environments. Exploring collaborative learning and improving robustness against adversarial attacks are also promising directions. Despite these strengths, the study is limited by the scope of the datasets used, which may not fully capture the diversity of real-world network traffic and emerging threats. Additionally, while the models show high accuracy, their performance in live, operational environments remains untested, and the black-box nature of some models may hinder their adoption without further efforts to enhance interpretability.

References

Al Mansur, A. and Zaman, T., (2023), November. User Behavior Analytics in Advanced Persistent Threats: A Comprehensive Review of Detection and Mitigation Strategies. In *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)* (pp. 1-6). IEEE. doi:https://doi.org/10.1109/isas60782.2023.10391553.

Al-Hashem, N. and Saidi, A. (2023). The Psychological Aspect of Cybersecurity: Understanding Cyber Threat Perception and Decision-Making. *International Journal of Applied Machine Learning and Computational Intelligence*, [online] 13(8), pp.11–22. Available at: https://neuralslate.com/index.php/Machine-Learning-Computational-I/article/view/41.

‌Andrade, R., Cazares, M. and Fuertes, W. (2021). Cybersecurity Attacks During COVID-19: An Analysis of the Behavior of the Human Factors and a Proposal of Hardening Strategies. *Springer eBooks*, pp.37–53. doi:https://doi.org/10.1007/978-3-030-71381-2\_3.

Baptiste Prébot, Du, Y. and González, C. (2023). Learning About Simulated Adversaries from Human Defenders using Interactive Cyber-Defense Games. *arXiv (Cornell University)*. doi:https://doi.org/10.48550/arxiv.2304.01142.

Bhardwaj, A., Kaushik, K., Alomari, A., Alsirhani, A., Alshahrani, M.M. and Bharany, S. (2022). BTH: Behavior-Based Structured Threat Hunting Framework to Analyze and Detect Advanced Adversaries. *Electronics*, [online] 11(19), p.2992. doi:https://doi.org/10.3390/electronics11192992.

Derbyshire, R., Green, B. and Hutchison, D. (2021). ‘Talking a different Language’: Anticipating adversary attack cost for cyber risk assessment. *Computers & Security*, 103, p.102163. doi:https://doi.org/10.1016/j.cose.2020.102163.

Dobson, G., Rege, A. and Carley, K. (2018). Informing Active Cyber Defence with Realistic Adversarial Behaviour. *Journal of Information Warfare*, [online] 17(2), pp.16–31. Available at: https://www.jstor.org/stable/26633151.

Egloff, F.J. and Smeets, M. (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, pp.1–32. doi:https://doi.org/10.1080/01402390.2021.1895117.

‌Hallett, J. (2019). *The Cyber Security Body of Knowledge*. [online] Available at: <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>.

Healey, J., Jenkins, N. and Work, J. (2020). Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations. *2020 12th International Conference on Cyber Conflict (CyCon)*. doi:https://doi.org/10.23919/cycon49761.2020.9131725.

Huang, C.-C., Huang, P.-Y., Kuo, Y.-R., Wong, G.-W., Huang, Y.-T., Sun, Y.S. and Meng Chang Chen (2022). Building Cybersecurity Ontology for Understanding and Reasoning Adversary Tactics and Techniques. doi:https://doi.org/10.1109/bigdata55660.2022.10021134.

Ilca, L.F., Lucian, O.P. and Balan, T.C. (2023). Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. *Sensors*, [online] 23(15), p.6757. doi:https://doi.org/10.3390/s23156757.

Izurieta, C. and Prouty, M. (2019). Leveraging SecDevOps to Tackle the Technical Debt Associated with Cybersecurity Attack Tactics. *2019 IEEE/ACM International Conference on Technical Debt (TechDebt)*. doi:https://doi.org/10.1109/techdebt.2019.00012.

Jabar, T. and Mahinderjit Singh, M. (2022). Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework. *Sensors*, 22(13), p.4662. doi:https://doi.org/10.3390/s22134662.

Jbair, M., Ahmad, B., Maple, C. and Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, 137, p.103611. doi:https://doi.org/10.1016/j.compind.2022.103611.

Jo, Y., Choi, O., You, J., Cha, Y. and Lee, D.H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors*, 22(5), p.1860. doi:https://doi.org/10.3390/s22051860.

‌Lahcen, R.A.M., Caulkins, B., Mohapatra, R. and Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, [online] 3(1). doi:https://doi.org/10.1186/s42400-020-00050-w.

Letteri, I., Della Penna, G., Di Vita, L. and Grifa, M.T., 2020, February. MTA-KDD'19: A Dataset for Malware Traffic Detection. In *Itasec* (pp. 153-165).

McCombie, S. (2018) ‘Threat actor oriented strategy: Knowing your enemy to better defend, detect and respond to cyber-attacks’, Journal of the Australian Institute of Professional Intelligence Officers. Woden, ACT: Australian Institute of Professional Intelligence Officers, 26(1), pp. 24–41. <https://search.informit.org/doi/10.3316/informit.630905164838114>.

Moallem, A. (2022). *HCI for Cybersecurity, Privacy and Trust: 4th International Conference, HCI-CPT 2022, Held as Part of the 24th HCI International Conference, HCII 2022, Virtual Event, June 26 – July 1, 2022, Proceedings*. [online] *Google Books*. Springer Nature.

Montasari, R., Hosseinian-Far, A. and Hill, R. (2018). Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments. *Advanced Sciences and Technologies for Security Applications*, pp.71–93. doi:https://doi.org/10.1007/978-3-319-97181-0\_4.

Muhammad Syafiq Kheruddin, Zuber, M. and Muhammad (2024). Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. doi:https://doi.org/10.22541/au.170534654.48067877/v1.

Munaiah, N., Rahman, A., Pelletier, J., Williams, L. and Meneely, A. (2019). Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition. *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*. doi:https://doi.org/10.1109/esem.2019.8870147.

Naseer, H., Maynard, S.B. and Desouza, K.C. (2020). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, p.113476. doi:https://doi.org/10.1016/j.dss.2020.113476.

‌Parmar, M. and Domingo, A. (2019). *On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander’s Understanding of the Adversary*. [online] IEEE Xplore. doi:https://doi.org/10.1109/MILCOM47813.2019.9020852.

Rich, M.S. (2023). Cyberpsychology: A Longitudinal Analysis of Cyber Adversarial Tactics and Techniques. 2(3), pp.618–655. doi:https://doi.org/10.3390/analytics2030035.

Rich, M.S. (2023). Enhancing Microsoft 365 Security: Integrating Digital Forensics Analysis to Detect and Mitigate Adversarial Behavior Patterns. *www.preprints.org*. [online] doi:https://doi.org/10.20944/preprints202306.1041.v2.

Roy, S., Sharmin, N., Acosta, J.C., Kiekintveld, C. and Laszka, A. (2022). Survey and Taxonomy of Adversarial Reconnaissance Techniques. *ACM Computing Surveys*. doi:https://doi.org/10.1145/3538704.

Sadrazamis, K. (2022). MITRE ATT&CK-based analysis of cyber-attacks in intelligent transportation. *Ihu.edu.gr*. [online] doi:https://repository.ihu.edu.gr//xmlui/handle/11544/30021.

Sarath, P. (2023) *Malicious traffic detection framework in internet of things using optimized linearly regressed deep CNN classifier*. In: *2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*2023/9/1-2023/9/2. IEEE.

‌Shaji, R.S., Sachin Dev, V. and Brindha, T. (2018). A methodological review on attack and defense strategies in cyber warfare. *Wireless Networks*, 25(6), pp.3323–3334. doi:https://doi.org/10.1007/s11276-018-1724-1.

Shukla, S. (2023). Synergizing Machine Learning and Cybersecurity for Robust Digital Protection. *Research Square (Research Square)*. doi:https://doi.org/10.21203/rs.3.rs-3571854/v1.

Subhan, D. and Lim, C. (2023). Analyzing Adversary’s Attack on Ethereum Collected from Honeypots. doi:https://doi.org/10.1109/icoict58202.2023.10262563.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y. and Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials*, pp.1–1. doi:https://doi.org/10.1109/comst.2023.3273282.