International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8459
***Article Received:** 24 July 2023 **Revised:** 12 September 2023 **Accepted:** 24 September 2023*

A Security Model for the Classification of Suspicious Data Using Machine Learning Techniques

Boussi Grace Odette[1], Himanshu Gupta[2], Syed Akhter Hossain[3]
[1]Ph.D. Scholar, AIIT
Amity University
Noida, India
graceboussi@gmail.com
[2]Professor, AIIT
Amity University
Noida, India
hgupta@amity.edu
[3]Professor, Computer Science and Engineering Department
University of Liberal Arts
Dhaka, Bangladesh
aktarhossain@daffodilvarsity.edu.bd

Abstract— Cybercrime first emerged in 1981 and gained significant attention in the 20th century. The proliferation of technology and our increasing reliance on the internet have been major factors contributing to the growth of cybercrime. Different countries face varying types and levels of cyber-attacks, with developing countries often dealing with different types of attacks compared to developed countries. The response to cybercrime is usually based on the resources and technological capabilities available in each country. For example, sophisticated attacks involving machine learning may not be common in countries with limited technological advancements. Despite the variations in technology and resources, cybercrime remains a costly issue worldwide, projected to reach around 8 trillion by 2023. Preventing and combating cybercrime has become crucial in our society. Machine learning techniques, such as convolutional neural networks (CNN), recurrent neural networks (RNN), and more, have gained popularity in the fight against cybercrime. Researchers and authors have made significant contributions in protecting and predicting cybercrime. Nowadays, many corporations implement cyber defense strategies based on machine learning to safeguard their data. In this study, we utilized five different machine learning algorithms, including CNN, LSTM, RNN, GRU, and MLP DNN, to address cybercrime. The models were trained and tested using the InSDN public dataset. Each model provided different levels of trained and test accuracy percentages.

Keywords- cybercrime, cybersecurity algorithm, CNN, RNN, GRU, LSTM, machine learning, model.

I. INTRODUCTION

Cybercrime refers to illegal activities that are committed online using electronic devices. It has become a widespread and well-known issue, posing a major challenge globally. Cybercriminals target various sectors, with the financial industry being a prime focus due to the potential for monetary gain.

To protect sensitive data and prevent cyber-attacks, cybersecurity experts employ various techniques and methods. One effective approach is the use of machine learning (ML) and artificial intelligence (AI). These technologies have proven to be valuable tools in handling the complexities of cyber-attacks.

ML and AI algorithms and models have been integrated into existing security systems to enhance their effectiveness. These technologies have shown promising results in detecting and mitigating cyber threats. However, as financial organizations implement AI and ML for their own security, cybercriminals also leverage these tools to make their attacks more sophisticated and harder to detect [4].

Cyber-attacks result in significant financial losses for both countries and individuals on a daily basis. There is a wide range of cybercrimes orchestrated through the internet, including ransomware attacks and phishing scams [10]. Ransomware involves encrypting victims' data and demanding a ransom for its release. Phishing, on the other hand, is a prevalent form of social engineering where attackers trick individuals into revealing sensitive information [1].

Tracking and attributing the components of a cyber-attack to a specific threat actor pose significant challenges for cybersecurity systems [6]. Cybersecurity experts continuously

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8459
***Article Received:** 24 July 2023 **Revised:** 12 September 2023 **Accepted:** 24 September 2023*

work to improve their techniques in order to detect, prevent, and respond to cyber threats effectively.

It is important to note that cybercrime is categorized into three groups: infractions, felonies, and misdemeanors. These classifications are based on the severity of the offenses and the corresponding punishments associated with each type of crime [5].

Overall, cybercrime remains a global issue, and researchers and experts are constantly proposing new ideas and strategies to combat this evolving threat. The widespread adoption of technology and the growth of the digital era have created both opportunities and risks, and it is crucial to stay vigilant and employ effective cybersecurity measures to protect against cyber-attacks[2].

Machine learning is a subfield of artificial intelligence that involves developing algorithms and statistical models that enable computers to learn from data and make predictions or decisions without being explicitly programmed. It involves analyzing and interpreting large datasets to identify patterns, relationships, and anomalies, and using this information to train models that can make predictions or decisions in new, unseen data. Machine learning has applications in a wide range of fields, including natural language processing, image recognition, recommendation systems, and predictive analytics.

Convolutional Neural Networks (CNNs) are deep learning models specifically designed for analyzing visual data. They have achieved remarkable success in tasks such as image classification and object detection. Inspired by the human visual cortex, CNNs learn and extract relevant features through convolutional layers and filters. These layers capture patterns at different spatial scales, enabling the detection of edges, textures, and other image features. Pooling layers down sample the output, making the network more robust and efficient. Deep CNN architectures consist of multiple convolutional and fully connected layers. Parameters are learned through backpropagation. CNNs have become fundamental in computer vision and image processing applications.

Recurrent Neural Networks (RNNs) are neural network architectures used for sequential data analysis. They utilize hidden states to capture dependencies and patterns in sequences, making them effective for tasks like language modeling and sentiment analysis. RNNs process inputs sequentially by combining current inputs with previous hidden states to generate outputs and update the hidden state. However, they suffer from the "vanishing gradient" problem, limiting their ability to capture long-term dependencies. To address this, variants like LSTM and GRU were introduced. Despite their limitations, RNNs are powerful models for sequential data analysis, achieving significant success in areas where context and temporal information are important.

LSTM (Long Short-Term Memory) is a type of recurrent neural network (RNN) architecture that excels at capturing long-term dependencies in sequential data. Unlike traditional RNNs, LSTM networks have an internal memory mechanism that allows them to selectively remember or forget information from previous time steps. This is achieved through three gates: forget, input, and output gates. LSTM is widely used in tasks such as speech recognition, machine translation, and sentiment analysis, where understanding and modeling long-term dependencies are crucial. By integrating LSTM layers into neural networks, models can effectively learn from and make predictions based on sequential data.

GRU (Gated Recurrent Unit) is an advanced type of recurrent neural network (RNN) architecture used in machine learning and deep learning. It overcomes the limitations of traditional RNNs by incorporating hidden states and two types of gates: update and reset gates. These gates allow the GRU to selectively retain and incorporate relevant past information, enabling it to capture long-term dependencies in sequential data effectively. GRUs have proven particularly effective in tasks involving sequential data, such as natural language processing and speech recognition. They are computationally efficient, capable of learning complex patterns, and widely used in various deep learning models.

MLP DNN stands for Multi-Layer Perceptron Deep Neural Network. In machine learning, MLP DNN is a type of neural network that uses multiple hidden layers to learn complex patterns in data. It is a popular choice for a variety of tasks, including image classification, speech recognition, and natural language processing.

II. LITERATURE REVIEW

The financial sector has widely embraced Machine Learning and Deep Learning techniques, which have become essential in facilitating activities like trading, mobile banking, payment processing, and credit decision-making for customers. [11]. According to [3], machine learning and deep learning algorithms offer a significant advantage in crime prediction due to their ability to analyze large volumes of data and identify patterns in criminal behavior or activity.

“Reference [7] presents a method utilizing genetic algorithms and deep feedforward neural networks to detect and prevent cyber-attacks on the networked control center of a smart grid. The approach improves attack detection in a smart grid environment, addressing existing limitations and achieving accuracy, performance metrics, and a low false positive rate.

In a study conducted by [8], it was found that cyber attacks present numerous challenges due to their increasing frequency and complexity. The study evaluates the performance of deep neural networks (DNNs) and other machine learning classifiers

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8459
***Article Received:** 24 July 2023 **Revised:** 12 September 2023 **Accepted:** 24 September 2023*

on multiple malware datasets. DNNs perform well, especially on the KDDCup 99 dataset, and a scalable hybrid framework called scale-hybrid-IDS-AlertNet is proposed for real-time monitoring and proactive detection of cyber attacks.

In another study, [9] introduces a parallel neural joint model algorithm that effectively detects malicious URLs by leveraging innovative techniques to extract semantic and visual information.

Focusing on the banking sector, [12] explores the usage of data mining techniques for various tasks such as client segmentation, credit scoring, fraud detection, and prediction of cyber crimes. Novel techniques like K-Means clustering, Influenced Association Classifier, and J48 Prediction tree are implemented to analyze cyber crime datasets, aiming to enhance cyber crime prediction and prevention in the banking industry.

Addressing the increasing risks of cybercrime in Mobile Money Services (MMS) that offer financial inclusion in developing nations, [13] develops a predictive model using Machine Learning (ML) techniques to detect suspicious customers and prevent cyber threats in MMS. The study showcases the effectiveness of ML algorithms in securing mobile money services.

Furthermore, [14] highlights the effectiveness of data mining techniques, including AI-based technologies and ML algorithms, in the banking sector for identifying customers who may engage in fraudulent activities during the credit process.

"Reference [15] evaluates the performance of widely used machine learning techniques, such as deep belief network, decision tree, and support vector machine algorithms, in detecting various cyber threats like spam, intrusion, and malware in cyberspace.

Shifting towards IoT systems, [16] proposes a reinforcement learning-based network intrusion detection system using a deep Q-network (DQN) to detect cyber threats. The study demonstrates superior performance compared to other machine learning models.

In [17], a framework for cyber security is presented, utilizing a data mining technique and the J48 decision tree algorithm to extract attack patterns and build a prediction model with high accuracy for detecting and predicting cyber attacks.

With regard to anomaly detection, [18] introduces an online unsupervised deep learning approach that outperforms traditional methods in detecting anomalous network activity from system logs. The proposed model significantly reduces analyst workloads and effectively identifies insider threat events.

In the context of cybersecurity, [19] explores the application of deep learning techniques, such as convolutional neural networks (CNN) and recurrent neural networks (RNN). Their study demonstrates the successful utilization of DL techniques in cybersecurity applications, achieving high accuracy and precision. Future research aims to further improve deep learning methodologies for cybersecurity.

It is important to note that accessing security data for research purposes is often challenging or unachievable due to concerns related to finances, business operations, and national security.

III. CONCEPTS OF THE PROPOSED SYSTEM

The objective of this project is to analyze dataset, built and test five different models based on the InSDN database. The results of the testing phase show that the Convolutional Neural Network (CNN) model performed the best, achieving a test accuracy rate of 92% on your dataset.

Given this high level of accuracy, using the CNN model to classify new data can be an effective approach to determine whether the data is suspicious or not. The model has demonstrated its capability to accurately classify data based on the patterns it has learned during the training process.

It is important to note that the accuracy of the model may vary depending on the distribution and characteristics of the new data. It is recommended to continuously monitor the performance of the model and retrain it regularly to ensure that it remains accurate and effective in classifying suspicious data.

IV. DATA PREPROCESSING

In the training phase of our data, we made the decision to remove certain features that could potentially impact the accuracy of our system. These features were identified to be irrelevant or potentially causing noise in the data.

Specifically, features such as Flow ID, Destination ID, Destination Port, and Time Stamp were removed in order to create our final dataset. By removing these features, we aimed to focus on the most informative and relevant aspects of our data that would contribute to building an accurate algorithm.

The goal of removing these features is to enhance the performance of the algorithm by reducing any potential noise or irrelevant information. By doing so, we can streamline the learning process and ensure that the algorithm is focusing on the most significant features that can effectively classify and analyze the data.

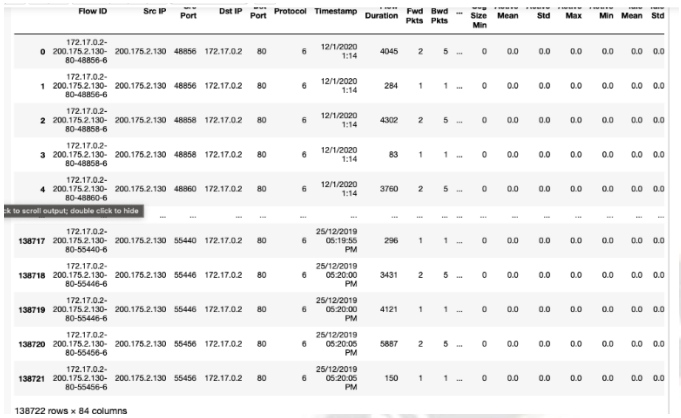
A. Data Set

We have used the publicly available InSDN dataset for our training and testing phase. The InSDN dataset consists of data related to network traffic and is used for various cybersecurity analysis tasks. In our case, we have identified six classes within the dataset: BFA, DDoS, DoS, Probe, U2R, and Normal. These classes represent different types of network attacks or normal network behavior.

To train and test our models, we likely considered various features available in the dataset. These features include attributes

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8459
***Article Received:** 24 July 2023 **Revised:** 12 September 2023 **Accepted:** 24 September 2023*

such as source IP address, destination IP address, timestamp, protocol type, packet length.



	Flow ID	Src IP	Src Port	Dst IP	Dst Port	Protocol	Timestamp	Flow Duration	Fwd Pkts	Bwd Pkts	...	Pkt Size Min	Pkt Size Mean	Pkt Size Std	Pkt Size Max	Pkt Size Min	Pkt Size Mean	Pkt Size Std
0	172.17.0.2-200.175.2.130-80-48856-6	200.175.2.130	48856	172.17.0.2	80	6	12/1/2020 1:14	4045	2	5	...	0	0.0	0.0	0.0	0.0	0.0	0.0
1	172.17.0.2-200.175.2.130-80-48856-6	200.175.2.130	48856	172.17.0.2	80	6	12/1/2020 1:14	284	1	1	...	0	0.0	0.0	0.0	0.0	0.0	0.0
2	172.17.0.2-200.175.2.130-80-48858-6	200.175.2.130	48858	172.17.0.2	80	6	12/1/2020 1:14	4302	2	5	...	0	0.0	0.0	0.0	0.0	0.0	0.0
3	172.17.0.2-200.175.2.130-80-48858-6	200.175.2.130	48858	172.17.0.2	80	6	12/1/2020 1:14	83	1	1	...	0	0.0	0.0	0.0	0.0	0.0	0.0
4	172.17.0.2-200.175.2.130-80-48860-6	200.175.2.130	48860	172.17.0.2	80	6	12/1/2020 1:14	3760	2	5	...	0	0.0	0.0	0.0	0.0	0.0	0.0
ck to scroll output; double click to hide	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
138717	172.17.0.2-200.175.2.130-80-55440-6	200.175.2.130	55440	172.17.0.2	80	6	25/12/2019 05:19:55 PM	296	1	1	...	0	0.0	0.0	0.0	0.0	0.0	0.0
138718	172.17.0.2-200.175.2.130-80-55446-6	200.175.2.130	55446	172.17.0.2	80	6	25/12/2019 05:20:00 PM	3431	2	5	...	0	0.0	0.0	0.0	0.0	0.0	0.0
138719	172.17.0.2-200.175.2.130-80-55446-6	200.175.2.130	55446	172.17.0.2	80	6	25/12/2019 05:20:00 PM	4121	1	1	...	0	0.0	0.0	0.0	0.0	0.0	0.0
138720	172.17.0.2-200.175.2.130-80-55456-6	200.175.2.130	55456	172.17.0.2	80	6	25/12/2019 05:20:05 PM	5887	2	5	...	0	0.0	0.0	0.0	0.0	0.0	0.0
138721	172.17.0.2-200.175.2.130-80-55456-6	200.175.2.130	55456	172.17.0.2	80	6	25/12/2019 05:20:05 PM	150	1	1	...	0	0.0	0.0	0.0	0.0	0.0	0.0

138722 rows × 84 columns

Figure 1. Dataset [20]

B. Pre-Process data set

After dropping the unwanted features from the dataset, several changes were made to preprocess the data before training the models. One of these changes involved converting the labels, which originally represented the traffic as either "normal" or "unnormal", into indexes. This means that instead of explicitly mentioning "normal" or "unnormal" in the code, they are represented by the indexes 1 and 2, respectively.

Furthermore, to ensure the randomness and unbiasedness of the data, it was shuffled before initiating the training process. Shuffling the data helps to avoid any systematic patterns or biases that may exist in the original order of the dataset.

During the training steps of the different algorithms, various metrics were measured to assess the performance of the models. Two important metrics that were calculated during the testing steps were the test loss and test accuracy.

The test loss quantifies how well the model is performing on unseen data by measuring the difference between the predicted outputs and the actual labels. A lower test loss indicates better performance.

The test accuracy, on the other hand, measures the proportion of correctly classified instances in the test dataset. It indicates how accurately the model is able to predict the correct labels for the given data.

	Train loss:	Train accuracy:	Test loss:	Test accuracy:
count	5.000000	5.000000	5.000000	5.000000
mean	0.772900	0.525380	1.017120	0.525320
std	0.393996	0.236713	0.396667	0.239541
min	0.348900	0.369300	0.446800	0.368400
25%	0.369300	0.380700	0.855600	0.377400
50%	0.866300	0.381200	1.129900	0.378200
75%	1.137500	0.576000	1.134700	0.579200
max	1.142500	0.919700	1.518600	0.923400

Figure 2. Data Pre-processed

C. Accuracy obtained after Testing:

After dividing the data into three parts - training, testing, and validation - we evaluated the accuracy of different models. The training and validation datasets were derived from the same data source.

Examining the accuracy results, we can assess the performance of each model. This analysis allows us to understand how well the models have learned from the training data and how effectively they can generalize their knowledge to predict on unseen data.

By comparing the accuracy of the models, you can identify which model performed best in terms of accurately classifying the data. This information is valuable for selecting the most reliable and effective model to use in further stages or for future predictions.

It is crucial to regularly evaluate the accuracy of models on unseen data to ensure their reliability and validate their usefulness for real-world applications. The figure below presents the accuracy results obtained for the different models:

	Model	Train loss:	Train accuracy:	Test loss:	Test accuracy:
0	CNN	0.3489	0.9197	0.4468	0.9234
1	LSTM	1.1375	0.3807	1.1299	0.3774
2	RNN	0.8663	0.5760	0.8556	0.5792
3	GRU	1.1425	0.3812	1.1347	0.3782
4	MLP DNN	0.3693	0.3693	1.5186	0.3684

Figure 3. Trained Accuracy and Test Accuracy result of Each Models

D. Result

After processing the tests using different Epochs, we obtained results for each algorithm. These results varied across the algorithms. In our case, the CNN algorithm had the highest accuracy compared to the other algorithms. Based on this better

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8459
***Article Received:** 24 July 2023 **Revised:** 12 September 2023 **Accepted:** 24 September 2023*

result, we have chosen to focus on and attach only the result of the CNN algorithm, which demonstrated the highest accuracy. By providing the results of the CNN algorithm, we have highlighted its performance and emphasizing its superiority compared to the other algorithms tested. This indicates that the CNN algorithm is most reliable for our specific task and dataset and can be trusted to accurately classify and analyze data for suspicious activity.

It is important to note that the accuracy of each algorithm can vary with different datasets and tasks. By sharing the results of the CNN algorithm, we are demonstrating its effectiveness and suggesting that it should be prioritized and considered for further analysis and implementation in the context of cybersecurity.

```
| Train loss: 0.3552 | Train accuracy: 0.9196 |
| Test loss: 0.3897 | Test accuracy: 0.9221 |
Epoch 98 took 2.72 seconds

| Epoch 100/100 |
| Train loss: 0.3489 | Train accuracy: 0.9197 |
| Test loss: 0.4468 | Test accuracy: 0.9234 |
Epoch 99 took 2.35 seconds

Training CNN model took 241.03 seconds
```

Figure 4. Result of CNN Model

V. DISCUSSION AND VISUALIZATION

After training the data using the five different algorithms (CNN, LSTM, RNN, GRU, and DNN), we obtained varying results in terms of test accuracy. The figure below visually depicts the test accuracy of each algorithm.

It is apparent from the figure that there is a significant difference in the test accuracy values among the five algorithms. This suggests that each algorithm performs differently on the given dataset.

The variation in test accuracy can be attributed to several factors. Firstly, different algorithms have unique architectures and learn different patterns from the data. This means that they may excel in different aspects of the dataset, leading to variations in accuracy. Additionally, the dataset itself may contain certain patterns or characteristics that are better suited to some algorithms compared to others.

It is important to consider these differences in test accuracy when selecting an appropriate algorithm for a particular task. The algorithm with the highest test accuracy may be the most suitable choice for your specific use case, as it has demonstrated the ability to accurately classify the data based on the patterns it has learned during training.

Further analysis and evaluation can help to determine the strengths and weaknesses of each algorithm and aid in making informed decisions about which algorithm to use in different scenarios.

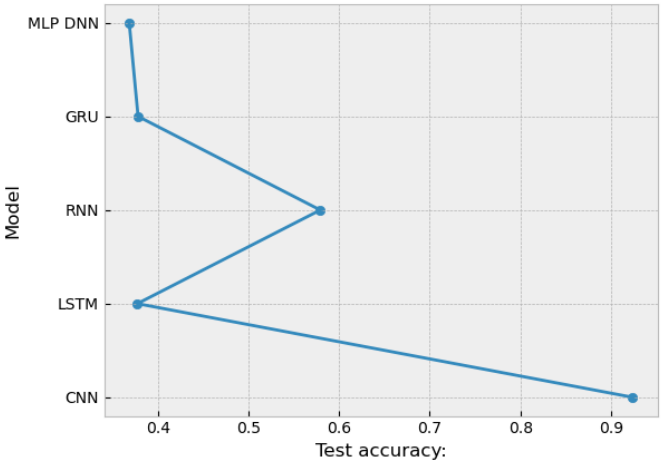


Figure 5. Plot Representation

VI. CONCLUSION AND FUTURE SCOPE:

With the increasing prevalence of cybercrime worldwide, machine learning has emerged as a crucial tool in providing security and combating cyber threats. In our study, after creating various machine learning algorithms, it was found that the Convolutional Neural Network (CNN) algorithm achieved the highest accuracy rate of 92%.

This high accuracy rate indicates that if new data is inserted into the CNN algorithm, there is a 92% chance that the algorithm will accurately classify the data as suspicious or not. The CNN algorithm has been trained to effectively learn and analyze patterns from the dataset, allowing it to make reliable predictions and identify potential threats.

As for the future scope of our work, one possible avenue is to create a prediction model using your CNN algorithm. By applying this algorithm to new and unseen data, we can evaluate its predictive capabilities and assess its performance in accurately predicting whether certain data points are suspicious or not.

Continuing to refine and enhance the algorithm, along with ongoing monitoring of its performance, can contribute to the development of more effective and robust prediction models in the field of cybersecurity. This can aid in proactive threat detection and prevention, helping to better safeguard against cybercrime.

REFERENCES

[1] Mughaid A, AlZu'bi S, Hnaif A, Taamneh S, Alnajjar A, Elsoud EA. An intelligent cyber security phishing detection system using deep learning techniques. Cluster Computing. 2022 Dec;25(6):3819-28.

[2] Arshey M, Viji KA. Thwarting cyber crime and phishing attacks with machine learning: a study. In2021 7th

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8459
***Article Received:** 24 July 2023 **Revised:** 12 September 2023 **Accepted:** 24 September 2023*

international conference on advanced computing and communication systems (ICACCS) 2021 Mar 19 (Vol. 1, pp. 353-357). IEEE.

[3] Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions

[4] Bilen A, Özer AB. Cyber-attack method and perpetrator prediction using machine learning algorithms. PeerJ Computer Science. 2021 Apr 9;7:e475.

[5] Saeed RM, Abdulmohsin HA. A study on predicting crime rates through machine learning and data mining using text. Journal of Intelligent Systems. 2023 Mar 31;32(1):20220223.

[6] Lazar D, Cohen K, Freund A, Bartik A, Ron A. IMDoC: identification of malicious domain campaigns via DNS and communicating files. IEEE Access. 2021 Mar 18;9:45242-58.

[7] Simonthomas S, Subramanian R. Detection and Prevention of Cyber-Attacks in Cyber-Physical Systems based on Nature Inspired Algorithm. In2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS) 2023 Feb 9 (pp. 483-487). IEEE.

[8] Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S. Deep learning approach for intelligent intrusion detection system. Ieee Access. 2019 Apr 3;7:41525-50.

[9] Yuan J, Chen G, Tian S, Pei X. Malicious URL detection based on a parallel neural joint model. IEEE Access. 2021 Jan 6;9:9464-72.

[10] Karim A, Shahroz M, Mustofa K, Belhaouari SB, Joga SR. Phishing Detection System Through Hybrid Machine Learning Based on URL. IEEE Access. 2023 Mar 3;11:36805-22.

[11] Nicholls J, Kuppa A, Le-Khac NA. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access. 2021 Dec 8;9:163965-86.

[12] Lekha KC, Prakasam S. Data mining techniques in detecting and predicting cyber crimes in banking sector. In2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) 2017 Aug 1 (pp. 1639-1643). IEEE.

[13] Sanni ML, Akinyemi BO, Akinwuyi D, Olajubu EA, Aderounmu GA. A Predictive Cyber Threat Model for Mobile Money Services. Annals of Emerging Technologies in Computing (AETiC). 2023 Jan 1;7(1):40-60.

[14] Biswas A, Deol RS, Jha BK, Jakka G, Suguna MR, Thomson BI. Automated Banking Fraud Detection for Identification and Restriction of Unauthorised Access in Financial Sector. In2022 3rd International Conference on Smart Electronics and Communication (ICOSEC) 2022 Oct 20 (pp. 809-814). IEEE.

[15] Shaukat K, Luo S, Chen S, Liu D. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In2020 international conference on cyber warfare and security (ICCWS) 2020 Oct 20 (pp. 1-6). IEEE.

[16] Rookard C, Khojandi A. Applying Deep Reinforcement Learning for Detection of Internet-of-Things Cyber Attacks. In2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) 2023 Mar 8 (pp. 0389-0395). IEEE.

[17] Rahman MA, Al-Saggaf Y, Zia T. A data mining framework to predict cyber attack for cyber security. In2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA) 2020 Nov 9 (pp. 207-212). IEEE.

[18] Tuor A, Kaplan S, Hutchinson B, Nichols N, Robinson S. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. arXiv preprint arXiv:1710.00811. 2017 Oct 2.

[19] Barik K, Misra S, Konar K, Fernandez-Sanz L, Koyuncu M. Cybersecurity deep: approaches, attacks dataset, and comparative study. Applied Artificial Intelligence. 2022 Dec 31;36(1):2055399.

[20] https://aseados.ucd.ie/datasets/SDN/