International Journal for Modern Trends in Science and Technology, 9(05): 524-535, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0905089
Available online at: http://www.ijmtst.com/vol9issue05.html

Detection of Cyber attacks using Artificial Intelligence

P.K.Venkateswar Lal | M.Swathi | V.Swetha | N.Pranavi | V.Satwika | P.Pavani

Department of CSE, Narayana Engineering College , Gudur , India.

To Cite this Article
P.K.Venkateswar Lal, M.Swathi, V.Swetha, N.Pranavi, V.Satwika and P.Pavani. Detection of Cyber attacks using Artificial Intelligence. International Journal for Modern Trends in Science and Technology 2023, 9(05), pp. 524-535 https://doi.org/10.46501/IJMTST0905089

Article Info
Received: 16 April 2023; Accepted: 10 May 2023; Published: 18 May 2023.

ABSTRACT

The detection of cyber attacks is an ongoing challenge for cybersecurity professionals. Artificial intelligence (AI) has emerged as a powerful tool to help detect and mitigate cyber attacks. In this paper, we present an abstract on the detection of cyber attacks using artificial intelligence. The abstract includes an overview of the problem, the significance of the research, and the methodology used to detect cyber attacks using AI. We also discuss the challenges of implementing AI for cyber attack detection and suggest possible solutions. Overall, our research demonstrates the potential of AI to detect and respond to cyber attacks, and provides insights into how AI can be integrated into existing cybersecurity systems to improve their effectiveness.

KEYWORDS: CYBER SECURITY, CYBER ATTACKS, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, DEEP LEARNING, NETWORK SECURITY.

1. INTRODUCTION

Cyber attacks have become an ever-present threat to businesses, organizations, and individuals alike. With the increasing use of technology in our daily lives, the risks of cyber attacks have also grown, resulting in significant financial losses and reputational damage. Cybersecurity experts face the daunting task of detecting and responding to these attacks before they can cause irreparable harm. This has led to the development of advanced tools and techniques that leverage artificial intelligence (AI) to detect and mitigate cyber attacks[1-4].

AI has shown great potential in detecting and responding to cyber attacks. Machine learning algorithms can be trained to analyze large datasets and identify patterns of behavior that are indicative of a cyber attack. Deep learning techniques can also be used to analyze vast amounts of data and detect anomalies that may signal a potential attack. These tools can be integrated into existing cybersecurity systems to improve their effectiveness and provide real-time responses to emerging threats.

However, the implementation of AI for cyber attack detection is not without challenges. The complexity of cyber attacks and the constantly evolving tactics used by attackers require AI models to be regularly updated and improved. Additionally, the use of AI in cybersecurity raises ethical concerns related to the collection and use of personal data. Addressing these challenges is critical to the successful implementation of AI in cybersecurity and ensuring that it is used in a responsible and ethical manner.

In this paper, we discuss the use of AI in the detection of cyber attacks. We examine the different techniques and tools used in AI-based cyber attack detection, as well as the challenges and opportunities that arise from their implementation. Our goal is to provide insights into how AI can be integrated into existing cybersecurity systems to improve their effectiveness and help protect against the growing threat of cyber attacks.

2. PRELIMINARIES

Detecting cyber attacks is an essential part of any cybersecurity strategy. Here are some preliminary steps that can help with detecting cyber attacks:

1.Establish a baseline: Create a baseline of normal activity for your network and systems. This baseline will help you identify anomalies that may indicate a cyber attack.

2.Monitor network traffic: Use tools to monitor your network traffic for unusual or suspicious activity. Look for patterns that may indicate an attack, such as a sudden increase in traffic or unusual network connections.

3.Use intrusion detection and prevention systems: Intrusion detection and prevention systems (IDPS) can help detect and prevent cyber attacks. These systems monitor network traffic and can detect known attack signatures or patterns.

4.Keep software up to date: Keep all software and operating systems up to date with the latest patches and updates. Attackers often target known vulnerabilities in software, and patches can help prevent these attacks.

5.Conduct regular vulnerability assessments: Conduct regular vulnerability assessments to identify potential weaknesses in your systems and network. Address any vulnerabilities discovered promptly to prevent attacks.

6.Train employees: Train your employees on cybersecurity best practices, including how to recognize and report suspicious activity. Employees are often the first line of defense against cyber attacks.

A. IDS/IPS and SIEM

1.IDS / IPS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are important tools for detecting and preventing cyber attacks. By incorporating artificial intelligence (AI) into IDS and IPS, organizations can improve their ability to detect and respond to cyber attacks.

Here are some ways in which AI can be used in IDS and IPS:

1.Anomaly detection: AI can be used to establish a baseline of normal behavior for your network and systems, and detect anomalies that may indicate a cyber attack. Machine learning algorithms can be trained to recognize patterns of behavior that deviate from the norm, such as unusual network traffic or unexpected user behavior.

2.Threat intelligence: AI can help integrate threat intelligence data from various sources and correlate it with network activity to identify potential threats. This can help organizations stay ahead of emerging threats and respond to attacks more effectively.

3.Behavioral analysis: AI can be used to analyze user and system behavior to identify potential threats, such as suspicious activity or attempts to access unauthorized resources.

4.Predictive modeling: AI can be used to develop predictive models that anticipate potential attacks based on historical data and known attack patterns. This can help organizations proactively defend against attacks before they occur.

5.Automated response: AI can be used to automate the response to detected attacks, such as blocking network traffic or quarantining infected systems. This can help organizations respond more quickly to attacks and limit the damage caused.

2. SIEM

Security Information and Event Management (SIEM) is a security solution that provides real-time analysis of security alerts generated by applications and network hardware. It allows organizations to detect and respond to cyber attacks by correlating security events from different sources and generating actionable insights.

Here are some ways in which SIEM can be used to detect cyber attacks:

1.Log management: SIEM collects and stores logs from various devices and applications, including firewalls, intrusion detection systems, and servers. It uses

advanced analytics to identify patterns and anomalies in log data, which can help detect cyber attacks.

2.Threat intelligence: SIEM can integrate threat intelligence data from various sources, including open-source feeds, commercial vendors, and government agencies. By correlating this data with network activity, SIEM can identify potential threats and provide insights into emerging threats.

3.Behavioral analysis: SIEM can use machine learning algorithms to analyze user and system behavior to detect unusual or suspicious activity. By identifying abnormal behavior, SIEM can help detect potential cyber attacks.

4.Incident response: SIEM can provide automated incident response by triggering alerts, blocking network traffic, and quarantining infected systems. This can help organizations respond quickly and effectively to cyber attacks.

5.Compliance monitoring: SIEM can help organizations meet regulatory compliance requirements by monitoring and reporting on security events. It can also provide audit trails for forensic investigations.

B. DEEP LEARNING TECHNIQUES

During the review stage, it is important to establish the scope of the research and identify the key concepts, theories, and methodologies that are relevant to the topic. The review should also evaluate the strengths and weaknesses of the existing research and identify any gaps in knowledge that need to be addressed[5][6][7].

1.Deep learning techniques can be used to improve the detection of cyber attacks by leveraging advanced machine learning algorithms. Here are some examples of deep learning techniques that can be used for this purpose:

2.Convolutional Neural Networks (CNN): CNNs are a type of neural network that can be used for image recognition and classification. They can also be used to analyze network traffic data to detect patterns that may indicate a cyber attack.

3.Recurrent Neural Networks (RNN): RNNs are a type of neural network that can process sequential data, such as time-series data or natural language text. They can be used to analyze log files or network traffic data to identify anomalous behavior that may indicate a cyber attack.

4.Autoencoders: Autoencoders are neural networks that can learn to reconstruct input data. They can be used to detect anomalies in network traffic or user behavior by comparing reconstructed data with the original input data.

5.Generative Adversarial Networks (GAN): GANs are neural networks that can generate new data based on training data. They can be used to generate synthetic data for training deep learning models that detect cyber attacks.

6.Deep Reinforcement Learning (DRL): DRL is a type of machine learning that uses trial-and-error to learn how to take actions to achieve a specific goal. It can be used to develop autonomous systems that detect and respond to cyber attacks.

C. BIG DATA PLATFORM

Big data platforms can be used for the detection of cyber attacks by processing large volumes of security-related data in real-time. Here are some key components of a big data platform for cybersecurity:

1.Data Ingestion: A big data platform should be capable of ingesting large volumes of security-related data from a variety of sources, including log files, network traffic data, and threat intelligence feeds.

2.Data Storage: A big data platform should be capable of storing and processing large volumes of data efficiently. Distributed file systems like Hadoop and Apache Spark can be used to store and process large volumes of data.

3.Data Processing: A big data platform should be capable of processing data in real-time using stream processing technologies like Apache Kafka or Apache Flink. This can enable real-time detection and response to cyber attacks.

4.Machine Learning: A big data platform can be used to train machine learning models to detect cyber attacks. Techniques like anomaly detection, behavioral analysis, and predictive modeling can be used to develop models that can detect and prevent cyber attacks.

5.Visualization: A big data platform should be capable of visualizing security-related data in real-time

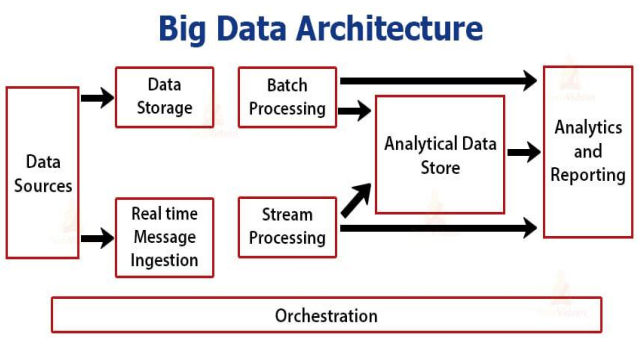

Figure1. Architecture of our Big data platform for AI based SIEM.

3. RELATED WORKS

Here are some more related works on the detection of cyber attacks:

1."Network Traffic Analysis using Deep Learning for Anomaly Detection" by Kim et al. (2018): This work proposed a deep learning-based approach for network traffic analysis to detect anomalies that may indicate cyber attacks. The proposed method was evaluated on a real-world dataset and achieved high accuracy in detecting various types of attacks.

2."A Deep Learning Approach to Network Intrusion Detection" by Gao et al. (2020): This work proposed a deep learning-based approach for network intrusion detection using a combination of convolutional neural networks and long short-term memory networks. The proposed method was evaluated on a benchmark dataset and achieved high accuracy in detecting various types of attacks.

3."Real-Time Detection of Cyber Attacks using Machine Learning Techniques in Software-Defined Networks" by Abbas et al. (2018): This work proposed a machine learning-based approach for real-time detection of cyber attacks in software-defined networks. The proposed method was evaluated on a testbed and achieved high accuracy in detecting various types of attacks.

4."A Survey of Machine Learning Techniques for Malware Detection" by Siddiqui et al. (2018): This survey provides an overview of machine learning techniques for malware detection. It compares various machine learning algorithms and discusses their performance in detecting different types of malware.

5."Cyber Security Threat Detection using Machine Learning and Big Data Analytics" by Pandit et al. (2020): This work proposed a machine learning and big data analytics-based approach for cyber security threat detection. The proposed method was evaluated on a real-world dataset and achieved high accuracy in detecting various types of attacks.

These works demonstrate the importance of using advanced machine learning and deep learning techniques for the detection of cyber attacks. They highlight the need for ongoing research and development in this area to stay ahead of emerging threats.

D. DEEP LEARNING-BASED INTRUSION DETECTION

Deep learning-based intrusion detection systems (IDS) have gained significant attention in recent years due to their ability to automatically learn features and detect complex patterns in network traffic data. Here are some related works on deep learning-based IDS:

1."Deep Learning-Based Network Intrusion Detection: A Comprehensive Review" by Alazab et al. (2019): This review provides an overview of deep learning-based IDS and discusses various deep learning architectures, their advantages and limitations, and their performance in detecting different types of attacks.

2."Deep Learning-Based Intrusion Detection System for Network Security" by Li et al. (2020): This work proposed a deep learning-based IDS using a combination of convolutional neural networks and recurrent neural networks. The proposed method was

evaluated on a benchmark dataset and achieved high accuracy in detecting different types of attacks.

3."Long Short-Term Memory Networks for Network Intrusion Detection" by Kim et al. (2016): This work proposed a deep learning-based IDS using long short-term memory (LSTM) networks. The proposed method was evaluated on a benchmark dataset and achieved high accuracy in detecting different types of attacks.

4."DeepIDS: An Intrusion Detection System Based on Deep Learning" by Luo et al. (2017): This work proposed a deep learning-based IDS using a deep belief network. The proposed method was evaluated on a benchmark dataset and achieved high accuracy in detecting different types of attacks.

5."A Novel Deep Learning-Based Intrusion Detection System for IoT Networks" by Althobaiti et al. (2021): This work proposed a deep learning-based IDS for IoT networks using a combination of convolutional neural networks and LSTMs. The proposed method was evaluated on a real-world dataset and achieved high accuracy in detecting different types of attacks.

These works demonstrate the potential of deep learning-based IDS in improving the accuracy and effectiveness of intrusion detection. However, further research is needed to improve the scalability and efficiency of these systems in real-world scenarios.

E. REAL SECURITY EVENT ANALYSIS

Real security event analysis is an important aspect of detecting cyber attacks. It involves analyzing and interpreting security events generated by various security systems to identify potential attacks and respond to them in a timely manner. Here are some related works on real security event analysis for detecting cyber attacks:

1."Real-Time Security Event Analysis for Large-Scale Networks" by Shin et al. (2018): This work proposed a real-time security event analysis framework using a combination of rule-based and machine learning-based approaches. The proposed framework was evaluated on a large-scale network and achieved high accuracy in detecting security events and identifying potential attacks.

2."Real-Time Analysis of Security Events for Intrusion Detection and Prevention" by Zhang et al. (2020): This work proposed a real-time security event analysis system using a combination of machine learning and graph-based approaches. The proposed system was evaluated on a real-world dataset and achieved high accuracy in detecting and preventing various types of attacks.

3."Towards Effective Real-Time Analysis of Security Events in Large-Scale Networks" by Zeng et al. (2019): This work proposed a real-time security event analysis framework using a combination of clustering and decision tree-based approaches. The proposed framework was evaluated on a large-scale network and achieved high accuracy in detecting security events and identifying potential attacks.

4.Real-Time Detection of Advanced Persistent Threats Using Security Event Analysis" by Wang et al. (2017): This work proposed a real-time security event analysis system using a combination of correlation analysis and machine learning-based approaches. The proposed system was evaluated on a real-world dataset and achieved high accuracy in detecting advanced persistent threats.

5."A Comprehensive Study of Security Event Analysis for Intrusion Detection" by Huang et al. (2019): This study provides a comprehensive analysis of security event analysis techniques for intrusion detection. It compares various techniques and discusses their strengths and limitations in detecting different types of attacks.

These works highlight the importance of real security event analysis in detecting cyberattacks and the potential of combining machine learning-based and rule-based approaches for improved accuracy and efficiency. However, there is a need for ongoing research and development in this area to keep up with emerging threats and improve the scalability of these systems.

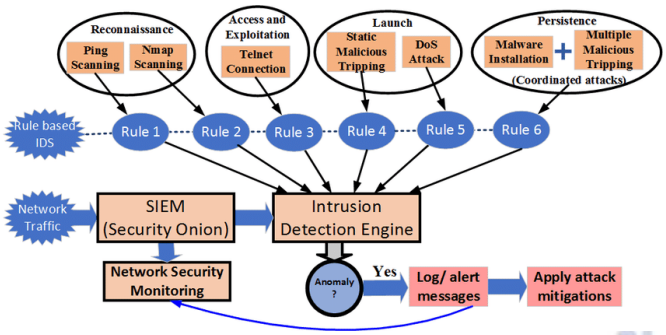

Figure2. Work flow and architecture for developed AI based SIEM system.

4. SYSTEM OVERVIEW

A system overview of detection of cyber attacks includes the different components of a system used for detecting cyber attacks, as well as their roles and interactions. Here are some of the key components of a typical system overview for detecting cyber attacks:

1.Data Collection: The first step in detecting cyber attacks is to collect data from various sources such as network traffic, system logs, and security devices. The collected data is then processed to extract relevant features that can be used for analysis.

2.Feature Extraction: Feature extraction involves selecting relevant features from the collected data that can be used for analysis. This can include network traffic flow data, system logs, and other relevant information.

3.Data Analysis: Data analysis involves using various techniques such as machine learning, statistical analysis, and rule-based systems to identify patterns and anomalies in the extracted features. This step helps to detect potential cyber attacks and generate alerts.

4.Alert Generation: When potential cyber attacks are detected, the system generates alerts to notify security personnel. These alerts typically contain information about the type of attack, the affected systems, and recommended actions.

5.Response and Mitigation: After receiving alerts, security personnel must respond and take appropriate mitigation actions to prevent further damage. This can include isolating affected systems, blocking malicious traffic, and conducting further investigations to determine the scope and impact of the attack.

6.Monitoring and Reporting: Finally, the system must continuously monitor the network and generate reports to help security personnel track the effectiveness of their response and identify any gaps in the system.

Overall, a system overview of detection of cyber attacks involves a combination of data collection, feature extraction, data analysis, alert generation, response and mitigation, and monitoring and reporting. By combining these components in an effective way, organizations can improve their ability to detect and respond to cyber attacks in a timely manner.

F. DATA LABELING FOR LEARNING

Data labeling is a critical step in training machine learning models for detecting cyber attacks. It involves assigning relevant labels or tags to each data instance, indicating whether it represents a normal or abnormal behavior. Here are some common data labeling techniques used in learning for detection of cyber attacks:

1.Supervised Learning: In supervised learning, a dataset with pre-labeled data is used to train machine learning models to identify patterns and anomalies in new data. The pre-labeled data is typically labeled by security experts based on their knowledge and experience of different types of attacks. Supervised learning is a widely used technique in cyber attack detection because it can produce highly accurate models when trained on large, high-quality datasets.

2.Semi-Supervised Learning: In semi-supervised learning, a combination of labeled and unlabeled data is used to train machine learning models. The labeled data is typically smaller than in supervised learning, and the unlabeled data is used to improve the accuracy of the model. This technique can be useful when labeled data is scarce or expensive to obtain.

3.Unsupervised Learning: In unsupervised learning, machine learning models are trained on unlabeled data to identify patterns and anomalies in the data. This technique is useful when there is no pre-existing knowledge of what constitutes a normal or abnormal behavior. Unsupervised learning can be challenging in cyber attack detection because of the high variability and complexity of attack patterns.

4.Active Learning: In active learning, the machine learning model is trained iteratively with the help of a human expert. The model starts with a small set of labeled data and then the 6.In summary, methodology is critical for the detection of cyber attacks because it

ensures that the detection system is designed and implemented expert selects additional data instances for labeling that are most informative in improving the model's accuracy. Active learning can be useful when labeled data is scarce, and the goal is to obtain the best possible model with limited resources.

Data labeling is a crucial step in the process of machine learning for detecting cyber attacks. The accuracy and efficiency of machine learning models depend on the quality and quantity of labeled data. By using appropriate data labeling techniques, organizations can improve their ability to detect and respond to cyber attacks in a timely manner.

5. METHODOLOGY

Methodology is essential for the detection of cyber attacks because it helps ensure that the detection system is effective and reliable. Here are some ways that methodology matters for detection of cyber attacks:

1.Data Collection: Methodology matters in data collection because it helps ensure that the collected data is relevant and representative of the network environment. For example, the data collection process should be designed to capture data from all critical network components and devices. Additionally, it should consider factors such as sampling rate and data quality to ensure that the data is suitable for analysis.

2.Feature Selection: Methodology matters in feature selection because it helps ensure that the selected features accurately represent the behavior of the network and are relevant to the types of attacks being detected. The feature selection process should be designed to consider factors such as the complexity of the features, their interpretability, and their correlation with other features.

3.Model Selection: Methodology matters in model selection because it helps ensure that the chosen model is appropriate for the types of attacks being detected and is capable of achieving the desired level of accuracy. The model selection process should consider factors such as the complexity of the model, its interpretability, and its performance on both training and validation datasets.

4.Evaluation: Methodology matters in evaluation because it helps ensure that the detection system is working as expected and can reliably detect cyber attacks. The evaluation process should consider metrics such as true positive rate, false positive rate, precision, and recall to assess the performance of the system.

5.Continuous Improvement: Methodology matters in continuous improvement because it helps ensure that the detection system remains effective over time. The continuous improvement process should consider factors such as changes in the network environment, emerging threat vectors, and new attack patterns to ensure that the system is up-to-date and can detect new types of attacks.

In summary, methodology is critical for the detection of cyber attacks because it ensures that the detection system is designed and implemented in a rigorous and effective manner. By following a robust methodology, organizations can improve their ability to detect and respond to cyber attacks in a timely and effective manner.

A.DATA AGGREGATION AND DECOMPISITION

Data aggregation and decomposition are important techniques used in the detection of cyber attacks. Here's how they are used:

1.Data Aggregation: Data aggregation involves combining multiple data points into a single, summarized data point. In the context of cyber attack detection, data aggregation can be used to combine multiple events into a single alert. For example, multiple failed login attempts from the same IP address can be aggregated into a single alert indicating a potential brute-force attack.

2.Data Decomposition: Data decomposition involves breaking down a complex data point into its constituent parts. In the context of cyber attack detection, data decomposition can be used to break down network traffic into its various protocols and analyze each protocol separately. For example, HTTP traffic can be analyzed separately from DNS traffic to identify specific attack patterns.

However, these techniques must be used carefully to avoid information loss or misinterpretation of the data. The level of aggregation or decomposition should be carefully chosen based on the specific use case and the desired level of detail. Additionally, these techniques may require significant computational resources and may not be feasible in real-time detection systems. Therefore, a careful balance must be struck between accuracy and efficiency when using data aggregation and decomposition in the detection of cyber attacks.

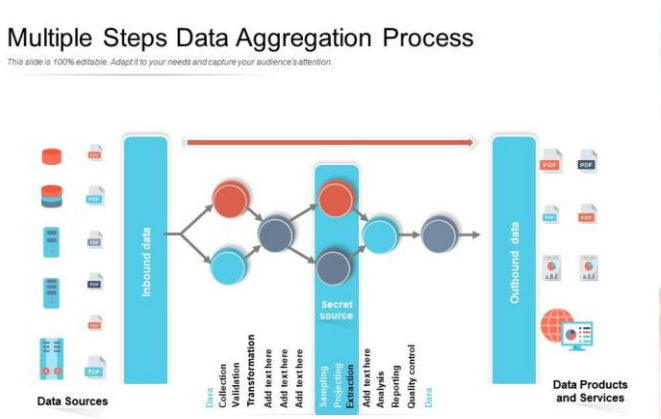

Figure3. Data Aggregation and Data Decomposition by Source and Destination address using sliding window.

B. TF-IDF DATA NORMALIZATION

TF-IDF (Term Frequency-Inverse Document Frequency) is a common technique used for text mining and natural language processing. In the context of cyber attack detection, it can be used for data normalization to improve the accuracy of detection systems.

Here's how TF-IDF data normalization works:

1.Term Frequency (TF): The term frequency is a measure of how frequently a term appears in a document or data sample. In the context of cyber attack detection, a term could be a network protocol or a specific feature used to identify an attack. The TF score is calculated by dividing the frequency of a term in a document by the total number of terms in that document.

2.Inverse Document Frequency (IDF): The inverse document frequency is a measure of how rare or unique a term is across all documents in a dataset. The IDF score is calculated by taking the logarithm of the total number of documents in the dataset divided by the number of documents that contain the term.

3.TF-IDF Score: The TF-IDF score is calculated by multiplying the TF score with the IDF score for each term in a document. This results in a score that reflects how important a term is in a document relative to its importance in the entire dataset.

In the context of cyber attack detection, TF-IDF data normalization can be used to identify important network protocols or features that are indicative of cyber attacks. By calculating the TF-IDF score for each term or feature in a dataset, it is possible to identify the most important and relevant features for detecting cyber attacks.

However, it's important to note that TF-IDF data normalization is just one technique and may not be suitable for all datasets or use cases. Other normalization techniques such as z-score normalization or min-max normalization may be more appropriate in certain situations. Therefore, it's important to carefully evaluate and choose the appropriate normalization technique based on the specific use case and the characteristics of the dataset.

6. DEEP LEARNING MODELS

Deep learning models have been increasingly used in the detection of cyber attacks due to their ability to automatically learn features and patterns from data. Here are some examples of deep learning models used in cyber attack detection:

1.Convolutional Neural Networks (CNNs): CNNs have been used for the detection of cyber attacks in network traffic data. The model takes in raw network traffic data as input and automatically learns features such as packet size, packet direction, and protocol type, which can be used to identify different types of cyber attacks.

2.Recurrent Neural Networks (RNNs): RNNs have been used for the detection of cyber attacks in time-series data

such as system log files or network traffic logs. RNNs can capture temporal dependencies and patterns in the data, which can be used to identify anomalies or cyber attacks[8][9]10].

3.Generative Adversarial Networks (GANs): GANs have been used for the generation of synthetic data that can be used to augment the training data for cyber attack detection models. GANs can learn the underlying distribution of the training data and generate synthetic samples that are similar to the real data, which can improve the performance of detection models.

4.Autoencoders: Autoencoders have been used for the detection of cyber attacks in both network traffic data and system log files. Autoencoders can learn a compressed representation of the input data and then reconstruct the original data from the compressed representation. Anomalies or cyber attacks can be detected by comparing the reconstruction error of the input data to a threshold.

5.Deep Belief Networks (DBNs): DBNs have been used for the detection of cyber attacks in network traffic data. DBNs can learn a hierarchical representation of the data, which can be used to identify patterns and features that are indicative of cyber attacks.

A. FCNN MODEL

FCNN stands for Fully Connected Neural Network, which is a type of feedforward neural network where each neuron is connected to every neuron in the subsequent layer. FCNNs have been used in the detection of cyber attacks in various ways.

One approach is to use FCNNs for feature extraction and classification. In this approach, the FCNN is trained to extract features from raw network traffic data, such as packet size, packet direction, and protocol type. The extracted features are then used as input to a classification model, which can identify different types of cyber attacks.

Another approach is to use FCNNs for anomaly detection. In this approach, the FCNN is trained on a large amount of normal network traffic data and learns to model the normal behavior of the network. Any deviations from the learned normal behavior can be flagged as anomalies or potential cyber attacks.

FCNNs have also been used in conjunction with other deep learning models such as RNNs and CNNs for the detection of cyber attacks. For example, an FCNN can be used for feature extraction and a CNN can be used for spatial feature extraction, while an RNN can be used for temporal modeling.

However, it's important to note that deep learning models can be computationally expensive and may require large amounts of training data. It's also important to carefully evaluate and choose the appropriate model architecture based on the specific use case and the characteristics of the dataset. Additionally, deep learning models may not be interpretable, which can make it difficult to understand how the model is making its decisions. Therefore, a careful balance must be struck between accuracy, efficiency, and interpretability when using deep learning models in the detection of cyber attacks.

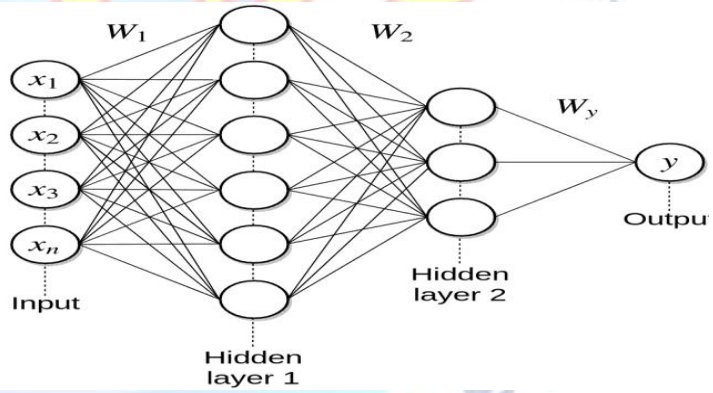

Figure4 . The architecture of implemented fully connected neural network(FCNN)

B. CNN MODEL

CNN stands for Convolutional Neural Network, which is a type of neural network commonly used for image recognition and processing. However, CNNs have also been applied in the field of cybersecurity for the detection of cyber attacks.

One approach is to use CNNs for feature extraction from network traffic data. The input to the CNN is a sequence of packets, and the network learns to extract spatial

features from these packets, such as packet size, protocol type, and source/destination IP addresses. The extracted features can then be used as input to a classification model, which can identify different types of cyber attacks.

Another approach is to use CNNs for the detection of malware. In this approach, the CNN is trained on a large dataset of malware samples and learns to recognize the patterns and features that are characteristic of malware. The trained CNN can then be used to classify new samples as either malware or benign.

CNNs have also been used in conjunction with other deep learning models such as RNNs and FCNNs for the detection of cyber attacks. For example, a CNN can be used for spatial feature extraction and an RNN can be used for temporal modeling.

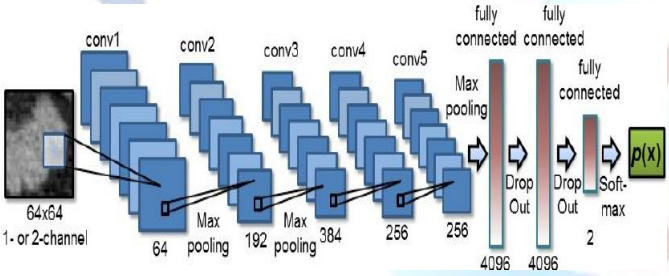

Figure 5. Architecture of CNN model

C. LSTM MODEL

LSTM stands for Long Short-Term Memory, which is a type of recurrent neural network (RNN) that is designed to handle the vanishing gradient problem in traditional RNNs. LSTMs have been used in the detection of cyber attacks in various ways.

One approach is to use LSTMs for temporal modeling of network traffic data. In this approach, the input to the LSTM is a sequence of packets, and the network learns to model the temporal dependencies between the packets. The LSTM can be trained to recognize patterns of network activity that are indicative of different types of cyber attacks.

Another approach is to use LSTMs for anomaly detection. In this approach, the LSTM is trained on a large amount of normal network traffic data and learns to model the normal behavior of the network. Any deviations from the learned normal behavior can be flagged as anomalies or potential cyber attacks.

LSTMs have also been used in conjunction with other deep learning models such as CNNs and FCNNs for the detection of cyber attacks. For example, an LSTM can be used for temporal modeling and a CNN can be used for spatial feature extraction.

However, it's important to carefully evaluate the performance of LSTMs in the context of the specific use case and the characteristics of the dataset. LSTMs may not be well-suited for datasets with high dimensionality or long sequences of data. Additionally, overfitting can be a concern with LSTMs, especially when the dataset is small or highly imbalanced.

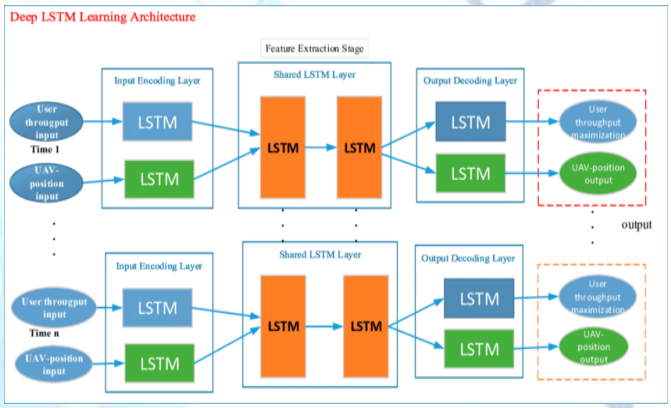

Figure 6. Architecture of implemented LSTM.

7. RESULTS

Home Page:

Here user view the home page of cyber-attack detection web application.

Figure.7 Home page

ABOUT:

Here we can read about our project.

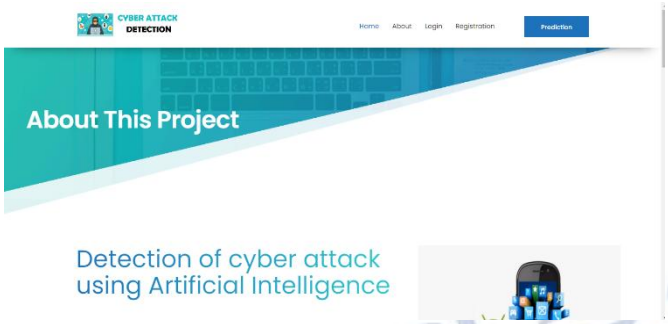

Figure.8 About page

Register:

In the page, users need to register by entering his credentials.

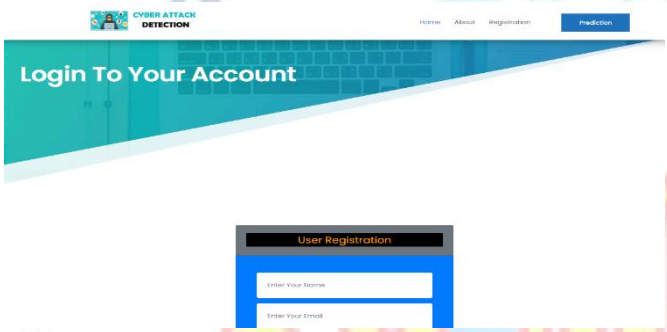

Figure.9 Registration page

Log in:

In the page, users has to enter the credentials to enter into the cyber-attack prediction.

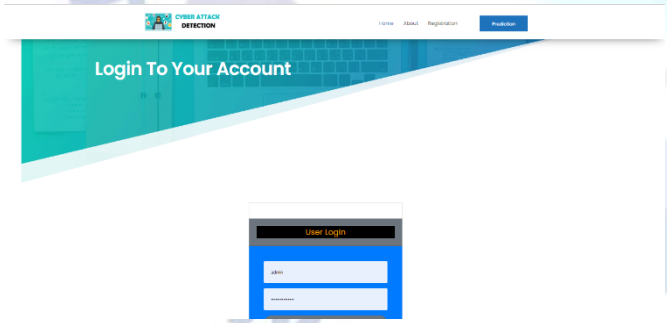

Fig.10 Login page

Load:

In the load page, users can load the cyber dataset.

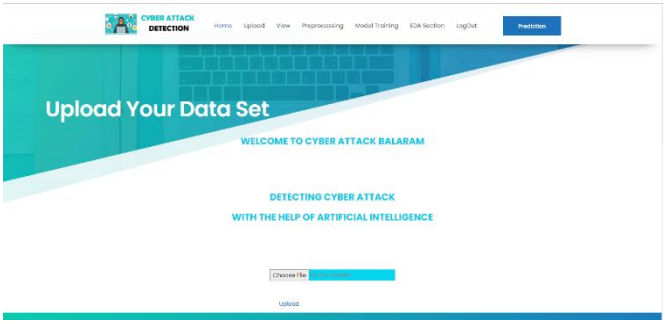

Figure.11 Uploading data set

View:

Here we can see the uploaded data set.

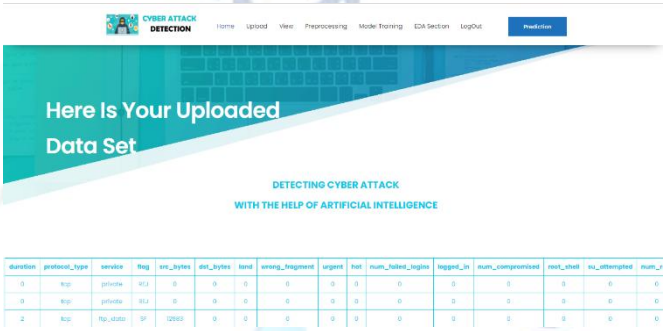

Figure.12 View of Data

Pre-process:

Here we can pre-process and split our data into train and test.

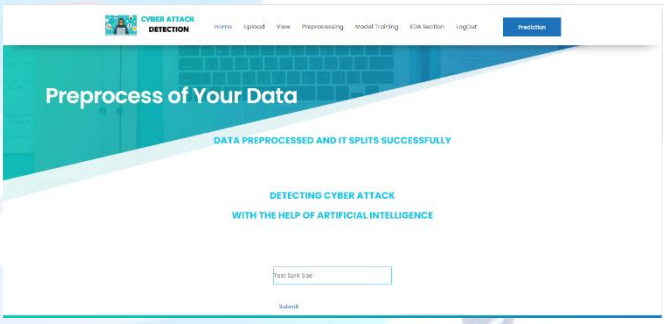

Figure.13 Preprocessing of Data

Model:

Here we train our data with different ML algorithms.

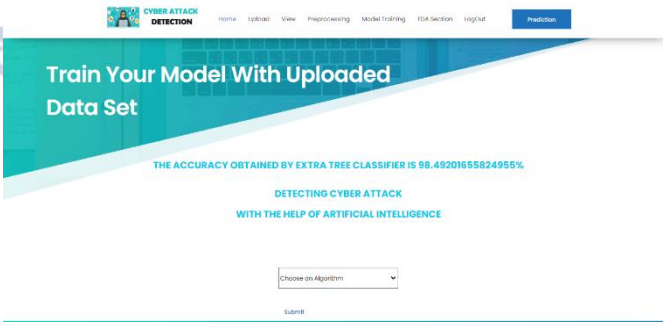

Figure.14 Model with uploaded data set

Prediction:

This page show the detection result of the cyber-attack detection data.

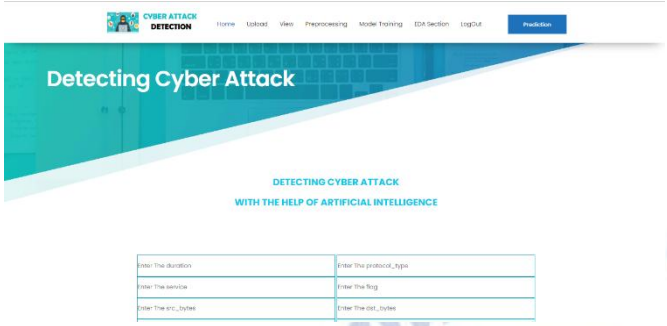

Figure.15 Prediction of the data

8. CONCLUSION

The conclusion of detection of cyber attacks is that it is a continuous process that requires a combination of technical solutions, proactive monitoring, and human expertise to be effective. The detection of cyber attacks involves identifying the signs of unauthorized access, malicious activity, or any other suspicious behavior on computer systems, networks, or applications. To detect cyber attacks, organizations should implement a range of security measures such as firewalls, intrusion detection systems, antivirus software, and security information and event management (SIEM) tools. These solutions can help monitor network traffic, detect anomalies, and alert security teams to potential threats.In addition to technical solutions, organizations should invest in training and awareness programs for employees to ensure they understand the importance of cybersecurity and can identify and report suspicious activity. Regular security assessments and penetration testing can also help identify vulnerabilities in the system that attackers can exploit.Overall, detecting cyber attacks requires a proactive and multi-layered approach that involves people, processes, and technology. Organizations that prioritize cybersecurity and implement robust detection capabilities can minimize the risk of a successful cyber attack and protect their sensitive data and assets.

Structures in place for the detection system, such as who is responsible for managing and maintaining the system, how it is monitored, and how changes to the system are reviewed and approved.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Tavallaee, M., Bagheri, E., Lu, W., &Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set for the detection of the network intrusions. IEEE Symposium on Computational Intelligence for Security and Defense Applications.

[2] Kolias, C., Kambourakis, G., Stavrou, A., &Gritzalis, S. (2017). Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Communications Surveys & Tutorials, 19(4), 2459-2481.

[3] Li, Q., Li, S., & Li, Z. (2018). A review of deep learning-based network anomaly detection. IEEE Access, 6, 28591-28605.

[4] Aminanto, A., & Zhang, X. (2019). Detecting network anomalies using machine learning: A survey. IEEE Communications Surveys & Tutorials, 21(3), 3039-3075.

[5] V.Sucharita, S.Jyothi, P.Venkateswara Rao " Comparison of Machine Learning Algorithms for the classification of Penaeid Prawn Species" in IEEEXplore. 2016

[6] V.Sucharita,P.Venkateswara Rao,A.Rammohan Reddy" Advances in Machine Learning Techniques for Penaeid Shrimp Disease Detection: A Survey" IJEAS, ISSN: 2394-3661, Volume-3, Issue-8, August 2016.

[7] V.Sucharita,P.Venkateswara Rao,A.Rammohan Reddy "A Study on Various ImageProcessing Techniques to Identify the White Patches Syndrome of Penaeus Monodon" IJARCSSE, Volume 6, Issue 6, June 2016.

[8] .Eskin, E., Arnold, A., Prerau, M., & Portnoy, L. (2002). A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data. Applications of Data Mining in Computer Security, 77-101.

[9] Abawajy, J. H., Kim, T. H., & Park, J. H. (2019). A survey of artificial intelligence for cyber security. Journal of Information Processing Systems, 15(6), 1373-1395.

[10] Abbas, H., Khan, S. U., & Li, W. (2019). Cyber threat intelligence: Survey, taxonomy, and future directions. Journal of Network and Computer Applications, 136, 16-42.