International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 17th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 12

DOI: 10.48047/IJIEMR/V11/ISSUE 12/30

Title **ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE**

Volume 11, ISSUE 12, Pages: 223-230

Paper Authors

Gunti Ramu, G. Narasimham

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE

1 Gunti Ramu, Mtech in Computer Networks and Information Security (CNIS) SIT JNTUH

2 G. Narasimham, Associate Professor, School of IT, JNTUH

ABSTRACT: Receptiveness is the general pattern on the grounds that the gamble of modern assaults has altogether expanded with the development of the Web and data innovation. Many firms have already put technology and services into place in an effort to offer the utmost visibility and defense against present-day risks. But without a multifaceted strategy, these efforts can be ineffective. Applications for large businesses are widely implemented and employ cloud technology. The usage of clouds is hastening the growth of the SDN industry. Increased network visibility is a major advantage of SDN networking. Traditional networks provide extensive security covering every aspect of traffic. SDN is detailed. Since it can assess danger knowledge information for different organization assaults, danger insight is a significant device for settling complex organization attacks, acquiring constant early admonition of dangers, and observing assaults. Based on research into machine learning, SDN, threat intelligence, central cloud networks, and other technologies. In this exploration, we work on the exactness of danger knowledge by utilizing profound learning and AI calculations. Simultaneously, we analyze the precision of different calculations that may successfully recognize assailants, assist us with getting ready for assaults, and shield us from hurt by uncovering their abilities.

Keywords *–machine learning, SDN, threat intelligence, central cloud networks*

1. INTRODUCTION

The industrialization and gathering application pattern of the Organization assault is clear given the current condition of safety. For specific lawbreaker gatherings, the organization has supplanted actual weapons as their primary apparatus or gear, and the assortments of organization dangers are more differed and complex. The ongoing security frameworks can't manage the extreme level, consistent, gathering, and weaponization dangers. Basic ventures and fundamental data foundation security network units have a wide landing impact and a high application limit, notwithstanding the way that they empower suitable discovery and insurance innovation. With the development of security intelligence, it is now possible to track security, provide early warning of risks, and deal with intricate network attacks in a simple yet efficient manner. Frameworks for modern control and the Web of things can access and control the two-way data trade between the creation organization and the Web straightforwardly or in a roundabout way. The organization assault plane has significantly expanded because of the pattern toward open interconnection, and the relating security cautious boundary likewise must be additionally extended. The foundation of a bunch of line constant advance notice and safeguard frameworks controlled by security knowledge, the opportune sharing of safety insight data, and the judicious utilization of danger knowledge are subsequently significant.

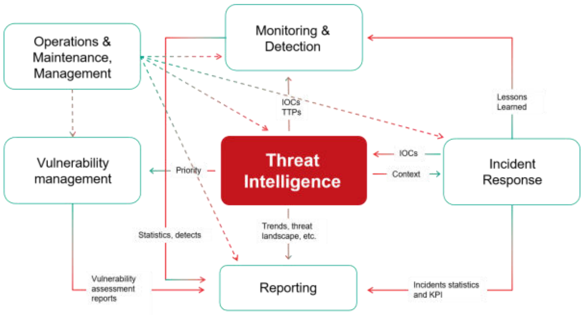


Fig.1: Example figure

Attackers who were formerly security nerds have changed into pros for whom cybercrime is a business. Their primary incentive for pursuing and assaulting any business is maximization of profit, which is determined even before the attack is launched. Since there are more and more different cyber threats, protecting networks is getting harder. While the majority of the threat intelligence models we now use were created using machine learning algorithms, it is necessary to explore deep learning techniques in order to improve accuracy, which is what we are doing in this work. The majority of targeted attacks combine social engineering with a set of specially created tools. A considerable decrease in the cost of conducting a successful targeted assault has coincided with a rise in the overall number of attacks worldwide. Of course, the goal is to attack as inexpensively as possible with the greatest financial results in order to reduce upfront expenditures. Platforms for threat intelligence combine threat intelligence feeds from many sources, automatically detect and stop new threats, provide security analytics, and integrate with other security products like SIEM, (next-gen firewalls) NGFWs, and EDR.

2. LITERATURE REVIEW

Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence :

Threat intelligence is the provision of evidence-based knowledge about existing or potential threats. Benefits of threat intelligence include improved efficiency and effectiveness in security operations in terms of detective and preventive capabilities. Successful threat intelligence within the cyber domain demands a knowledge base of threat information and an expressive way to represent this knowledge. This purpose is served by the use of taxonomies, sharing standards, and ontologies. This paper introduces the Cyber Threat Intelligence (CTI) model, which enables cyber defenders to explore their threat intelligence capabilities and understand their position against the ever-changing cyber threat landscape. In addition, we use our model to analyze and evaluate several existing taxonomies, sharing standards, and ontologies relevant to cyber threat intelligence. Our results show that the cyber security community lacks an ontology covering the complete spectrum of threat intelligence. To conclude, we argue the importance of developing a multi-layered cyber threat intelligence ontology based on the CTI model and the steps should be taken under consideration, which are the foundation of our future work.

Are we ready for SDN? Implementation challenges for software-defined networks:

Cloud services are exploding, and organizations are converging their data centers in order to take advantage of the predictability, continuity, and quality of service delivered by virtualization technologies. In parallel, energy-efficient and high-security networking is of increasing importance. Network operators, and service and product providers require a new network solution to efficiently tackle the increasing demands of this changing network landscape. Software-defined networking has emerged as an efficient network technology capable of supporting the dynamic nature of future network functions and intelligent applications while lowering operating costs through simplified hardware, software, and management. In this article, the question of how to achieve a successful carrier grade network with software-defined networking is raised. Specific focus is placed on the challenges of network performance, scalability, security, and interoperability with the proposal of potential solution directions.

Analyzing Malicious URLs using a Threat Intelligence System:

Threat intelligence and management systems form a vital component of an organization's cybersecurity infrastructure. Threat intelligence, when used with active monitoring of network traffic, can be critical to ensure reliable data communication between endpoints. Threat intelligence systems are well suited for analyzing anomalous behaviors in network traffic and can be employed to assist organizations in identifying and successfully responding to cyber-attacks. In this paper, we present a machine learning approach for clustering malicious uniform resource locators (URLs). We focus on a URL dataset gathered from a threat intelligence feeds framework. We implement a k-means clustering solution for grouping malicious URLs obtained from open source threat intelligence feeds. We demonstrate the effectiveness of our unsupervised learning technique to discover the hidden structures in the malicious URL dataset. Our URL keyword/text clustering solution provides valuable insights about the malicious URLs and aids network operators in policy decisions to mitigate cyber-attacks. The clusters obtained using our approach has a silhouette coefficient of 0.383 for a dataset containing over 11,000 malicious URLs. Lastly, we develop a probabilistic scoring model to calculate the percentage of malicious keywords present in a given URL. After analyzing over 72,000 malicious keywords, our model successfully identifies over 80% of the URLs in a test dataset as malicious.

Preventing Poisoning Attacks On AI Based Threat Intelligence Systems:

As AI systems become more ubiquitous, securing them becomes an emerging challenge. Over the years, with the surge in online social media use and the data available for analysis, AI systems have been built to extract, represent and use this information. The credibility of this information extracted from open sources, however, can often be questionable. Malicious or incorrect information can cause a loss of money, reputation, and resources; and in certain situations, pose a threat to human life. In this paper, we use an ensembled semi-supervised approach to determine the credibility of Reddit posts by estimating their reputation score to ensure the validity of information ingested by AI systems. We demonstrate our approach in the cybersecurity domain, where security analysts utilize these systems to determine possible threats by analyzing the data scattered on social media websites, forums, blogs, etc.

Using high-interaction networks for targeted threat intelligence:

Provided are methods, network devices, and computer-program products for targeted threat intelligence using a high-interaction network. In some implementations, a network device in a network may receive suspect network traffic. The suspect network traffic may include network traffic identified as potentially causing harm to the network. The network device may determine that the suspect traffic is associated with an unknown threat. The network device may further analyze the suspect network traffic using a high-interaction network. In various implementations, the high-interaction network may be configured to emulate at least a part of the network. In various implementations, analyzing the suspect network traffic may include determining a behavior of the suspect network traffic in the high-interaction network. The network device may further generate indicators, where the indicators may describe the suspect network traffic. In various implementations, the indicators facilitate analysis of a network's susceptibility to the unknown threat.

3. METHODOLOGY

The ongoing group, weaponization, and high-level threats pose a challenge to the current security systems. With a high application limit and expansive landing influence, a decent discovery and guard framework is upheld by significant ventures and basic data foundation security network units.

This study researches and fosters a functioning cautious instrument for cloud stages utilizing Danger Insight. We can understand the linkage insurance ability of the whole appropriated cloud community and foster a precise organization security early admonition and capture capacity at the cloud place's Web limit by investigating key innovations like enormous information savvy examination, multi-source Danger Insight Combination, and SDN innovation.

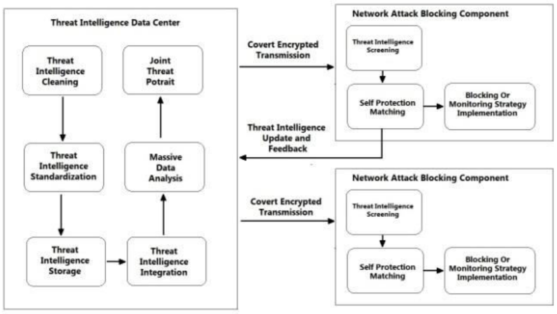

Threat Intelligence Data Center
Threat Intelligence Cleaning
Joint Threat Potrait
Threat Intelligence Standardization
Massive Data Analysis
Threat Intelligence Storage
Threat Intelligence Integration
Covert Encrypted Transmission
Threat Intelligence Update and Feedback
Covert Encrypted Transmission
Network Attack Blocking Component
Threat Intelligence Screening
Self Protection Matching
Blocking Or Monitoring Strategy Implementation
Network Attack Blocking Component
Threat Intelligence Screening
Self Protection Matching
Blocking Or Monitoring Strategy Implementation

Fig.2: System architecture

MODULES:

- **Upload train Dataset:** We'll submit a dataset to the programme.
- **Run preprocessing TF-IDF algorithm:** gives a phrase a value based on how significant it is.

- **Generate Event Vector:** The exception type must be determined by the processor before branching to the proper handler.

- **Neural Network Profiling:** We can examine our models graphically.

- **Run Algorithms:** We'll obtain accurate algorithms.

- **Accuracy comparison Graph:** The various algorithms' performance will be compared.

4. IMPLEMENTATION

The various algorithms' performance will be compared.

Svm algorithm:

One of the supervised ML methods used for both regression & classification problems is Support Vector Machine (SVM). Using a method known as the kernel trick, it converts your statistics before locating a superior boundary between the possible outcomes solely on the basis of those alterations.

Knn algorithm:

The k-nearest neighbors (KNN) method is another straightforward method for supervised machine learning that focuses primarily on regression and classification issues.

Random forest:

It creates several decision trees by randomly selecting samples, using their majority vote for classification and average for regression. It solves issues involving continuous variables in regression and difficulties involving categorical variables in classification, where the data set in question has both. It excels at classification-related issues.

Naïve bayes:

A directed learning method for characterizing gives that is dependent on the Bayes hypothesis is the Nave Bayes calculation. With a large training set, it is mostly used for text categorization. One of the most straightforward and effective classification techniques currently available is the Naive Bayes Classifier. It helps create quick machine learning models that can accurately predict the future. As a probabilistic classifier, it predicts the likelihood of an event occurring. A few common applications of Naive Bayes algorithms include article classification, sentiment analysis, and spam filtration.

Decision tree:

The managed learning calculation family incorporates the choice tree calculation. The choice tree strategy, as opposed to different techniques for directed learning, can manage issues connected with arrangement and relapse. In decision trees, we expect the class name of a record and start at the tree's root. A correlation is made between the upsides of the root characteristic and the record property.

Deep learning algorithms used

Cnn (convolutional neural network):

CNN primarily consists of several layers that are utilized for object detection, image processing, and zip code letter and digit identification.

CNN processes the data by running it through several layers and extracting the characteristics to display convolutional operations.

Lstm (long short-term memoy) algorithm

A unique variety of recurrent neural networks is the LSTM (RNN). These are designed with long-term dependency learning and adaptation in mind. It can remember and take into consideration more records for a longer period of time. Because they can limit previous inputs or memory inputs, LSTMs are primarily used in sequence predictions. They are designed to remember over time.

5. EXPERIMENTAL RESULTS

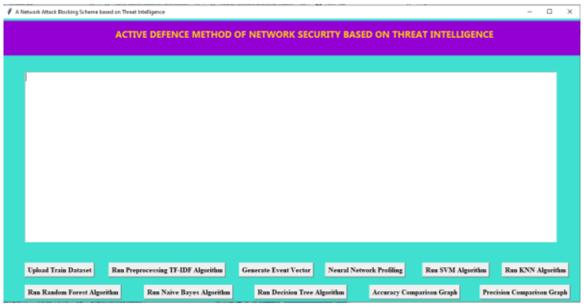
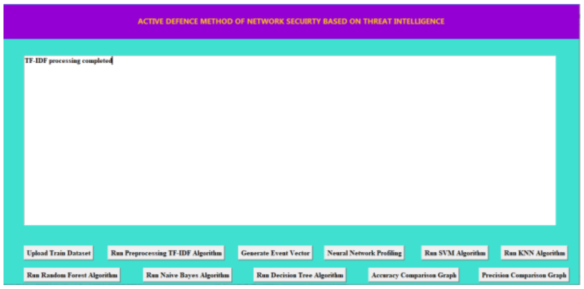
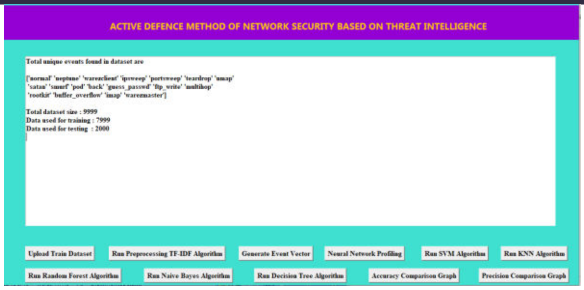

A Network Attack Blocking Scheme based on Threat Intelligence
ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

Fig.3: Home screen


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

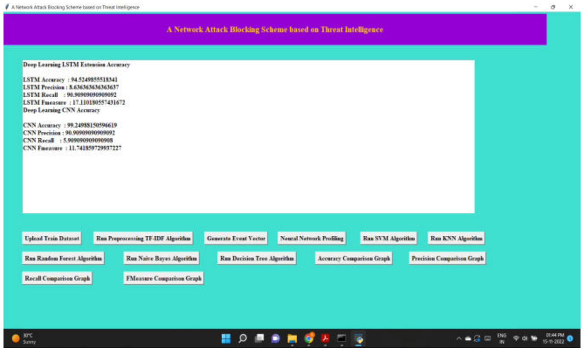
```
TF-IDF processing completed
```

Fig.4: TF-IDF algorithm


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

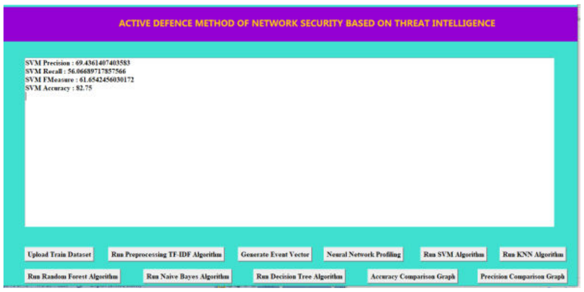
```
Total unique events found in dataset are

['normal' 'neptune' 'warezclient' 'ipsweep' 'portsweep' 'teardrop' 'nmap'
 'satan' 'smurf' 'pod' 'back' 'guess_passwd' 'ftp_write' 'multihop'
 'rootkit' 'buffer_overflow' 'imap' 'warezmaster']

Total dataset size : 9999
Data used for training : 7999
Data used for testing  : 2000
```

Fig.5: Generate event vector


A Network Attack Blocking Scheme based on Threat Intelligence
A Network Attack Blocking Scheme based on Threat Intelligence
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph
Recall Comparison Graph
FMeasure Comparison Graph
30°C
Sunny
ENG
IN
01:44 PM
15-11-2022

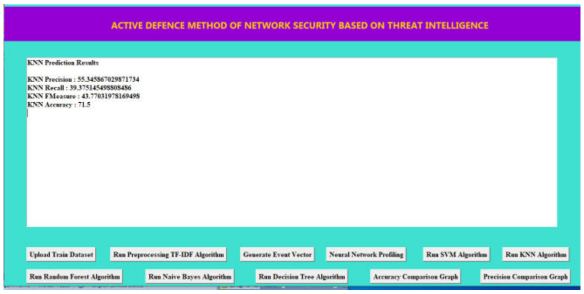
```
Deep Learning LSTM Extension Accuracy

LSTM Accuracy  : 94.5249855518341
LSTM Precision : 8.636363636363637
LSTM Recall    : 90.9090909090909092
LSTM Fmeasure  : 17.1101805574316672
Deep Learning CNN Accuracy

CNN Accuracy  : 99.24988150596619
CNN Precision : 90.90909090909092
CNN Recall    : 5.909090909090908
CNN Fmeasure  : 11.741859729937227
```

Fig.6: Neural network profiling


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

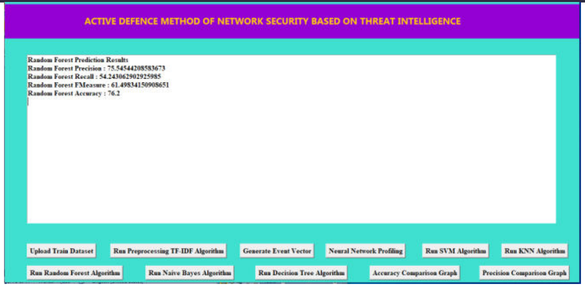
```
SVM Precision : 69.4361407403583
SVM Recall : 56.06689717857566
SVM FMeasure : 61.6542456030172
SVM Accuracy : 82.75
```

Fig.7: SVM algorithm


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

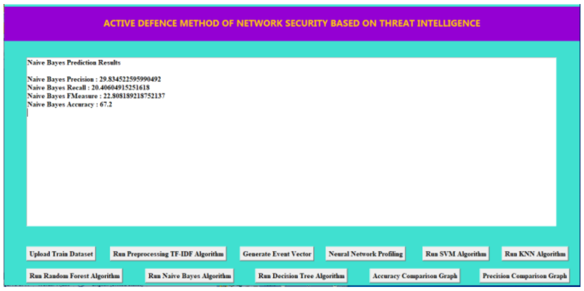
```
KNN Prediction Results

KNN Precision : 55.345867029871734
KNN Recall : 39.375145498808486
KNN FMeasure : 43.77031978169498
KNN Accuracy : 71.5
```

Fig.8: KNN algorithm


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

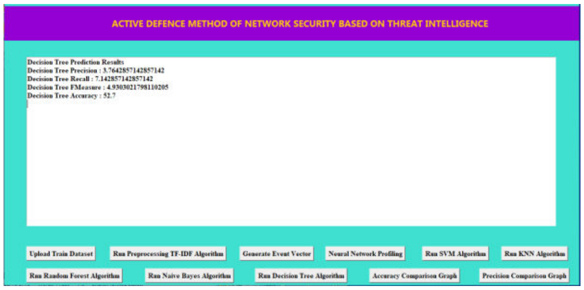
```
Random Forest Prediction Results
Random Forest Precision : 75.54544208583673
Random Forest Recall : 54.243062902925985
Random Forest FMeasure : 61.49834150908651
Random Forest Accuracy : 76.2
```

Fig.9: Random forest model


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

```
Naive Bayes Prediction Results

Naive Bayes Precision : 29.834522595990492
Naive Bayes Recall : 20.40604915251618
Naive Bayes FMeasure : 22.808189218752137
Naive Bayes Accuracy : 67.2
```

Fig.10: Naïve bayes model


ACTIVE DEFENCE METHOD OF NETWORK SECURITY BASED ON THREAT INTELLIGENCE
Upload Train Dataset
Run Preprocessing TF-IDF Algorithm
Generate Event Vector
Neural Network Profiling
Run SVM Algorithm
Run KNN Algorithm
Run Random Forest Algorithm
Run Naive Bayes Algorithm
Run Decision Tree Algorithm
Accuracy Comparison Graph
Precision Comparison Graph

```
Decision Tree Prediction Results
Decision Tree Precision : 3.7642857142857142
Decision Tree Recall : 7.142857142857142
Decision Tree FMeasure : 4.9303021798110205
Decision Tree Accuracy : 52.7
```

Fig.11: Decision tree algorithm

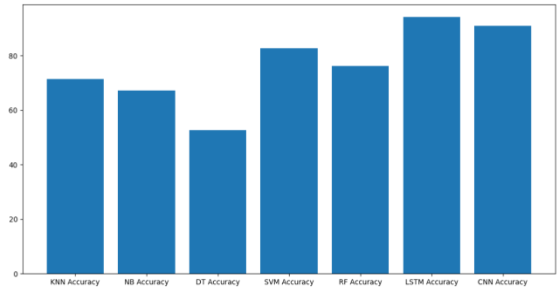


Fig.12: Accuracy comparison graph

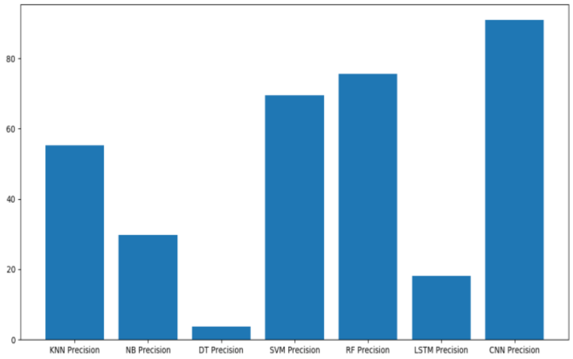


Fig.13: precision comparison graph

For this work, we utilized AI algorithms like SVM, KNN, Naive Bayes, and Decison Tree as well as neural network algorithms like CNN and LSTM to prepare and produce machine learning models. We then, at that point, made exactness and accuracy diagrams for every calculation with the end goal of correlation, as displayed in the charts above. We found that the CNN (Convolution Neural Network) a Deep Learning algorithm-based model has the most noteworthy accuracy with 99.53, while the LSTM (Long Short-Term Memory) profound learning model has the most elevated precision with 94.52

6. CONCLUSION

Using a variety of Windows-based and Python-based machine learning and deep learning methods, this study attempted to generate threat intelligence information models. This research effort has analyzed several algorithms and assessed their accuracy and precision through the study of threat intelligence processing technology. When comparing the results to one another, it is evident that CNN of Deep Learning algorithm has high precision of 99.43% and LSTM Deep Learning algorithm has much superior accuracy of 94.52% when compared to other algorithms. These findings clearly imply that, when compared to machine learning algorithms proposed in prior studies, any of the two Deep Learning models may be employed to increase effectiveness. These Deep learning-based Threat intelligence Information data centers are able to rapidly raise the total network security protection level and lessen the load on business applications' security protection.

REFERENCES

[1] Mavroeidis, V., & Bromander, S.. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE.

[2] Sezer S, Scott-Hayward S, Chouhan P, et al. Are we ready for SDN? Implementation challenges for software-defined networks[J]. IEEE Communications Magazine, 2013, 51(7):36-43.

[3] Nayak, S., Nadig, D., & Ramamurthy, B.. (2019). Analyzing Malicious URLs using a Threat Intelligence System. 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE.

[4] Khurana N, Mittal S, Piplai A, et al. Preventing Poisoning Attacks On AI Based Threat Intelligence Systems[C]// 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP). IEEE, 2019.

[5] Singh A, Gukal S. Using high-interaction networks for targeted threat intelligence[J]. 2019..

[6] Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. T.. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. Computers & Security, 67(JUN.), 35-58.

[7] Tax D M J, Duin R P W. Support vector domain description[J]. Pattern recognition letters, 1999, 20(11-13): 1191-1199.

[8] Xiaoyan R, Danwa S. Research on Cyber-Attack Defense System Based on Big Data and Threat Intelligence[J]. Journal of Information Security Research, 2019.

[9] S. Lee and T. Shon, Open source intelligence base cyber threat inspection framework for critical infrastructures, in 2016 Future Technologies Conference (FTC), Dec 2016, pp. 1030–1033.