CYBER THREAT DETECTION USING NEURAL NETWORKS AND MACHINE LEARNING

Mrs. Ch. Ramya Bharathi[1], L. Mounika[2], D. Amulya[3], L. Niteesh[4], D.Chinna Khasim[5]

[1]Assistant Professor, Department of CSE-Artificial Intelligence & Machine Learning , SRK Institute of Technology, Vijayawada
[2,3,4,5]Student, Department of CSE-Artificial Intelligence & Machine Learning , SRK Institute of Technology, Vijayawada

ABSTRACT

Detection techniques for cyberthreats can be so difficult, such as the provision of an efficient system for automated detection. The author develops one based on artificial neural networks, which are capable of detecting artificial intelligence-type cyberthreats by using deep learning rather than other AI methods. This approach transforms many security alerts obtained during the monitoring process into isolated event signatures, followed by a more comprehensive analysis to identify internet-related attacks with better results in comparison with conventional approaches. Our research produced an AI-SIEM that is a result combination of event profiling and various other neural network types like convolutional neural networks (CNNs), and artificial neural networks (ANNs) for handling data. The main significance is that it ensures fast reaction time by distinguishing genuine alerts from fake ones. All experiments in this study were carried out by the authors on two benchmark datasets (NSLKDD and CICIDS2017) and two actual datasets for comparison with other already existing methods. Their abilities were assessed using well-known machine-learning approaches to contrast them with other established performances; therefore, learning makes them an effective model for detecting network intrusions. It outperforms traditional technique methods on machine-learning grounds, even though it is used practically.

Keywords: Threat Detection, Neural Networks, Internet, Cyber Attacks

1. INTRODUCTION

In the digital era, the increase in the number and complexities of cybercrimes have made it a significant worry on the minds of many individuals. Oftentimes, the conventional signature-based intrusion detection systems (IDS) and security information and event management (SIEM) tools find it impossible to deal effectively with the changing terrain of cyber-attacks. To solve this problem, a lot of scientists are looking at more sophisticated machine learning models like AI, which help in detecting different types of information online that may be harmful to someone else.

A possible strategy among many would be to implement artificial neural networks (known as ANNs)—machine learning models inspired by the brain's architecture and functioning that are highly adept at recognising patterns, detecting anomalies, and predicting trends necessary for effective cyber threat detection. Security analysts can potentially enhance the accuracy and responsiveness of their cyber defense systems by using the strong feature extraction and non-linear modeling capabilities of ANNs. This paper introduces a new way of finding cyberthreats by using event profiling together with other ANN combinations such as FCNNs, CNNs, and LSTM. Evolved from artificial intelligence (AI), this security information and event management (SIEM) aims at enabling differentiating elements of a cyberattack from false alarms so that security teams may better respond to these developing dangers.

This study aims to:

- Preprocess security event data using event profiling to enhance ANN-based detection.
- Evaluate various ANN models (CNN and ANN) with respect to the identification of cyber threats, comparing them to conventional ML techniques.
- Present evidence supporting the use of the proposed method based on standardized as well as authentic cyber security data, highlighting its strength in detecting intrusions.

2. LITERATURE REVIEW

In the study paper, entitled "CYBER THREAT DETECTION BASED ON ARTIFICIAL NEURAL NETWORKS AND ML," a fresh technique for stepping up cyber attack recognition through artificial neural networks (ANNs) is proposed. The authors developed a security system that analyzes information related to security attacks, especially on computers. It is based on event profiling and different techniques, which include fully connected neural networks (FCNN), convolutional neural networks (CNN), and long short-term memory (LSTM) networks.

The key focus of this work is to improve the discrimination between true positive and false positive alerts, enabling security analysts to respond more effectively to emerging cyber threats. The authors evaluated the proposed ANN-based models using both benchmark (NSLKDD and CICIDS 2017) and real-world cybersecurity datasets and compared their performance to five traditional machine learning techniques (SVM, k-NN, Random Forest, Naive Bayes, and Decision Tree). The results demonstrated that the ANN-based methods outperformed the conventional ML approaches in terms of intrusion detection accuracy.

The literature review articles further explore how AI and ML are more extensively applied in cybersecurity. These studies offer a complete overview of AI-based solutions for different cybersecurity cases, like threat detection, vulnerability analysis, malware analysis, and incident response. For example, Akhtar et al.'s review categorizes the extant AI applications in the area of cybersecurity into six main headings: detecting threats, analyzing vulnerabilities, detecting malware, automated security, responding to incidents, and detecting intrusions. This domain is one that is very complex and may be difficult to understand completely. This is why the authors discuss the challenges that it presents as well as what it could inspire in researchers. If the existing and future AI systems were understandable enough, many other fields would benefit too. It was also mentioned that AI models should be interbred with human professionals in order to make good decisions during cyber security measures.

This paper also explores the role of security information and event management (SIEM) in responding to cybersecurity incidents. Holm et al. An in-depth review of existing research on SIEM tools was conducted and highlighted the need for public awareness to manage cybersecurity incidents. The authors introduce the concept of social-technical SIEM (ST-SIEM) methods, which consider both technical and social factors in problem solving.

In this regard, the literature examines the role played by security information and event management systems in the response to cybersecurity incidents. Holm et al.'s work offers an extensive exposition of existing studies on SIEM tools, which underscores the necessity for an all-rounded socio-technical approach towards managing cybersecurity events. They are suggesting the idea of a socio-technical SIEM (ST-SIEM) system that looks at both social and technical dimensions in responding to incidents.

In the reviewed literature, it's been shown that when dealing with the current challenges related to cybersecurity, the increasing significance of artificial intelligence (AI) and machine learning (ML) methods is being observed. A research document related to artificial neural network detection of cyber threats suggests that applying neural networks' pattern recognition features can lead to better precision and speediness in security surveillance systems.

3. EXISTED SYSTEM

The existing system of cyber threat detection is based on traditional signature-based approaches that look forward to the well-established templates of feasible assaults. These ways are generally not able to cope with an unknown or zero-day attack quarter, given that they lack any consideration for cyber threats that progress over time. The system already uses rule-based systems that are based on predefined rules and thresholds for identifying possible threats. These systems are characterized by their inability to adopt new threats as well as their reliance on human expertise in defining the rules.

When it comes to detecting cyber threats, existing methods basically use a signature-based detection, a rule-based system, and anomaly detection techniques:

- In Signature-Based Detection, incoming data packets or files are compared to a database of known attack signatures. Known threats are effectively mitigated with signature-based systems but new emerging threats that do not coincide with the existing signatures cannot be detected using these systems. However, this will work for any other kind of data.

- Rule-based systems are systems that are programmed with predetermined rules and thresholds by security experts, and these rules determine the course of action when certain conditions are met. However, such systems could be useful for established threats that have already been recognized lacking in adaptability to novel attack modes of operation if continually updated in line with constantly changing internet risks.

- Anomaly-based methods are meant for detecting any departure from the standard network behavior. The anomaly may indicate a threat if it is not a common pattern or activity in a network. Yet, their dependence on statistical thresholds causes a large number of false alarms and the benign anomalies are difficult to separate from real threats.

In addition, the present system is built around methods that detect unusual network traffic pattern variations. But these methods can generate wrong alerts and are not enough against advanced attacks that imitate the normal behavior of the network.

4. PROPOSED SYSTEM

The current system for cyber threat detection employs artificial intelligence in order to boost its detection features and tackle former systems' limitations.

- **Event Profiling and Deep Learning:**
  The suggested system undertakes preliminary processing of gathered security events. These are processed and input into several AI models such as Fully Connected Neural Networks (FCNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks. The system becomes capable of identifying already familiar and unfamiliar dangers as it reads the data deeply, which makes it understand intricate patterns and interconnections improved.

- **Adaptability and Learning:**
  Education and adaptability can be achieved through the ability to learn from certain training datasets with many security labels, thus changing and developing the detection mechanisms within our method. This means the method for detecting dangers will keep improving by acquiring fresh information.

- **Performance Evaluation:**
  The developers did a great job of running some tests on the system by using several standard data sets like the NSLKDD & CICIDS2017; as well as actual everyday situations, so that it could work efficiently. According to a comparison with conventional Machine Learning methods; such as SVMs (Support Vector Machines), k-NN (k-Nearest Neighbors), RFs (Random Forests), NB (Naive Bayes) and DTs (Decision Trees), performance evaluation reveals the superiority of the ANN-based model on IDS detection results in accuracy as well as false alarms frequency.

- **Integration and Scalability:**
  Harmonizing at any level with the present Security Information and Event Management (SIEM) systems; the project system is meant to be flexible enough. This means that it can be transformed into a robust security solution upon which the present ones could be built should the need arise. Therefore, the scalability and flexibility in design are critical components that will enable the project system to meet different industry requirements and also those of other entities within an industry.

Finally, the proposed system is a big step forward when it comes to detecting cyber threats and it does manage to do so through artificial neural networks and machine learning. It can surely be noted that it can be used for detecting threats that exist within a certain network since its focus lies in flexibility, precision as well as ability to grow- all indispensable components that are to help maintain secure cyberspace in this era of changing cyber risks.

5. METHODOLOGY

5.1. Data Collection and Preprocessing:

The first phase of our approach involves gathering and curating data that will be used to train neural network-based models as well as machine learning models that are later evaluated. The data consists of several types of cyber threat indicators, such as network traffic logs, system event logs, malicious software samples, and common types of attacks. The initial stage of our technique involves gathering data. This data can be put to use in order to develop neural network models and machine learning models, which will then need to be validated. Together with well-known attacks, this information carries different cyber threat indicators, including network traffic logs, system event logs, and malware samples.

5.2. Neural Network Architectures:

During this phase, we will consider different neural network architectures that are suitable for carrying out cyber threat detection functions. Such could be convolutional neural networks (CNNs), recurrent neural networks (RNNs), long-short-term memory (LSTM) networks, or hybrids developed specifically to meet certain data characteristics and detection requirements.

5.3. Machine Learning Algorithms:

Apart from the known fact that a processor with deep learning algorithms needs to be big enough to use neural networks, there are many other machine learning algorithms analyzed to detect cyber threats. These comprise decision trees, support vector machines (SVMs), k-nearest neighbors (k-NN), and random forests, as well as clustering algorithms and anomaly detection methods based on data point labels. In this light, every algorithm is tested on how well it generalizes from its training data while managing distinct kinds of digital security break-ins at different stages of their evolution.

Algorithms Used:

1. **Linear Regression:**

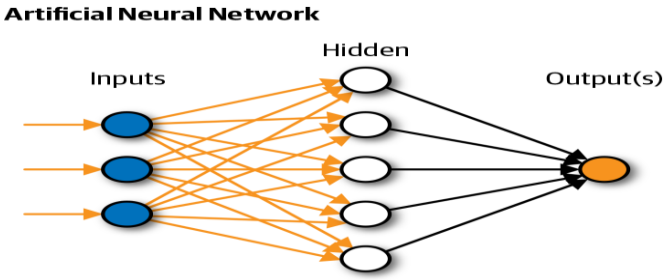
   Regression of linear sort is what we consider one of the fundamental algorithms in machine learning used to predict an output that is continuous using an input that has one or more features. The way it operates is that there is a straight-line formula attached to witnessed values and postulated data while striving to reduce total differences between postulated values and real data sets through minimization of square deviation. In economics, finance, and the social sciences, linear regression is commonly used for purposes such as forecasting sales, predicting house prices, and analyzing trends.

2. **Logistic Regression:**

   Logistic regression is specific to binary classification cases involving two possible outcomes in the target variable, unlike linear regression. It models the likelihood of an input belonging to some class by utilizing the logistic function that transforms inputs into values ranging from 0 to 1. Spam detection, disease diagnosis, and credit risk analysis are some applications where this algorithm has been widely applied.

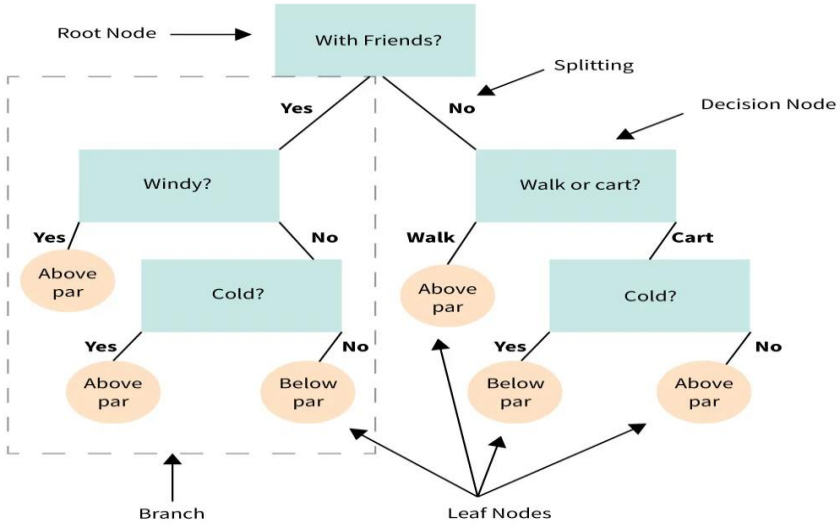
3. **Artificial Neural Networks:**

   Computational models referred to as artificial neural networks (ANNs) have been designed based on animal brain biological neural networks configuration and functionality. These networks have units which are closely related known as neurons that are capable of processing signals before transmitting them to other neighboring neurons. ANNs are usually arranged in hierarchies consisting of input caches that are hidden while some may be visible, but in either case allow the system to manage multiple modifications with each passing moment. Due to the fact that ANNs are able to model nonlinear processes and draw conclusions from intricate data sets, they are employed in a number of areas such as predictive modeling, adaptive control, artificial intelligence and others.these networks work on supervised learning principle whereby they learn from labeled training data adjusting parameters so that the predicted output becomes as close as possible within the limit set by actual one. In order to boost their accuracy over time, many machine learning and artificial intelligence applications resort to the use of training data.



4. Decision Trees:

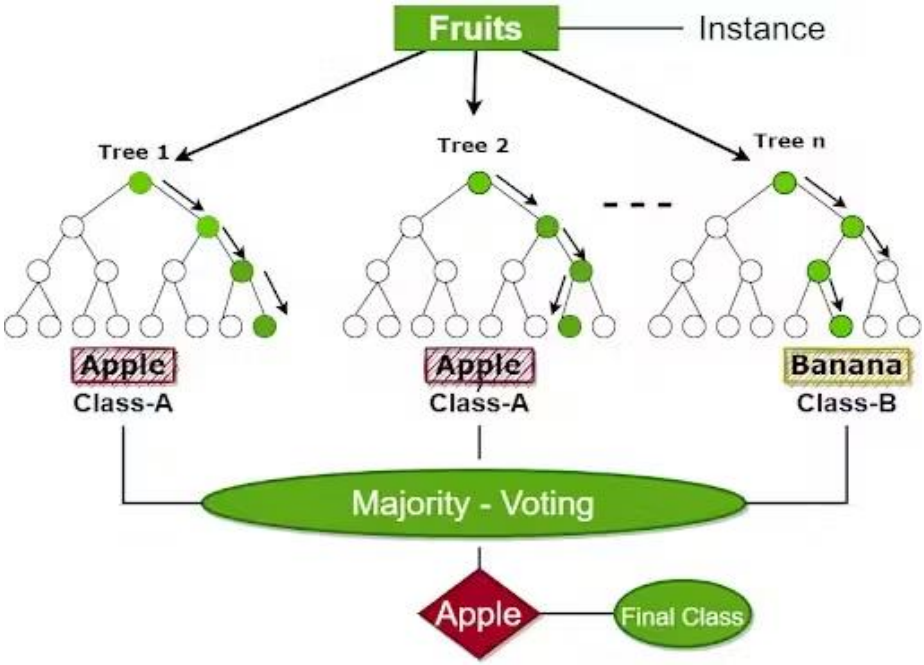
In supervised learning, Decision Trees can do classification as well as regression because they are flexible. To enhance the uniformity of the target variable within every distinct area, they



break down the input space into sections based on selected values of features. Among other uses, we use it in customer classification, fraud detection, and medical diagnosis because they are easy to use and easy to understand.

5. Random Forest:

The Random Forest is a method of ensemble machine learning algorithm that aims to enhance the prediction accuracy and robustness of decisions by combining a number of decision trees. Random Forest constructs multiple decision trees at random points in the training dataset and pools these trees for averaging (in the case of regression) or voting (in the case of classification). Random forest is a technique that is used in fields like finance, e-commerce, and healthcare to do, among other things, customer churn prediction, product recommendation, and disease diagnosis. This is because of its potential to handle elaborate data and avert overfitting.

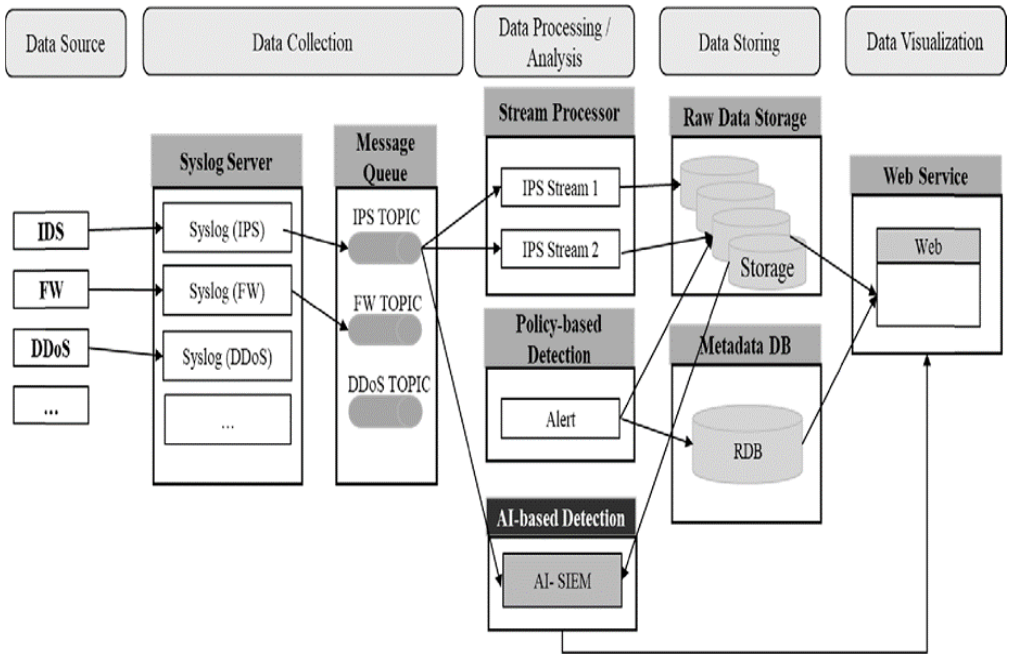


6. **Support Vector Machines(SVM):**
Support Vector Machines (SVM) are algorithms with high strength that can be used in classifying things and also in estimating numbers. It mainly aims at finding the best boundary line to separate the classes in the data space so that it maximizes the margin between them. This algorithm can be applied in different fields such as text categorization and image recognition, among others, due to its ability to deal with high-dimensional data and complex interrelations that are not linear, among others.

7. **k-Nearest Neighbors (k-NN):**
Classification and regression tasks require algorithms that are easy to understand and apply. One such algorithm is k-Nearest Neighbors(kNN); it is so simple that its pseudocode is often imprinted in the minds of first-year computer science students. Another example of this type of algorithm is Support Vector Machines (SVMs).

5.4. Feature Extraction and Selection Techniques:

The selection and extraction of features from datasets plays a pivotal role in maximizing the performance of machine learning models and neural networks in the disclosure of cyber threats. We, therefore, investigate different techniques regarding this area, which include statistical analysis as well as frequency domain analysis, among others.



6. FUTURE ENHANCEMENTS

Dynamic and sophisticated cyber threats require detection systems that continually improve. Integrations of neural networks and machine learning (ML) will advance future cyber threat detection, thereby enhancing the effectiveness and durability of security structures. The use of adversarial machine learning methods is one important area for development. Training models on recognising and preventing adversarial attacks can definitely increase the robustness of cybersecurity systems so that they will become more resistant to attempts at avoidance created by bad people. Another highly promising direction for improvement lies in the use of multimodal fusion methods that combine various data, e.g., network traffic, system logs, and user behaviors, to better understand what possible threats might exist. One can utilize neural networks in order to fuse and scrutinize these various streams of data, contributing to higher precision as well as the dependability of threat detection capabilities.

In the future, the development of explainable AI will be important as well. For instance, there may be a need for developing models that explain why they have taken particular decisions in order to improve the reliability and understanding of cyber threat detection systems. In respect to this, any given transparency promotes comprehension of any given output from artificial intelligence by safety experts, promoting better scrutiny in certification processes, especially when dealing with critical security-oriented apps. Federated Learning is a chance to enhance the detection of computer threats. Tracing threats in multiple entities where their information systems are not exposed to security breach can be among the ways this improvement might happen. Also, through this technique, it is possible to come up with systems capable of detecting threats much better than those that already exist and, at the same time, keep the sources unknown when they were obtained in their separate sovereign states. Intelligent self-learning methods need to be designed that can identify potential threats increasingly with the interaction tempo in online platforms. This regularly updates their policies and decision-making procedures through various environmental pull-pin strategies, so that they can efficiently remain one step ahead of arising dangers from time to time.

Major advancements in progress in quantum computing hold out the possibility of substantial improvement in performance due to the rise of quantum-inspired algorithms for detecting cyber threats. These new algorithms could outstrip classical methods in both efficiency and effectiveness at accommodating highly complicated contemporary cyber threats. Should include automatic threat response into the cybersecurity detection tools. Acceleration and enhancement of threat prevention can be achieved in this way: automatic mechanisms of response, such as quarantine, network reconfiguration, or deployment of defensive countermeasures, should be implemented. The cyber threat detection models' long-term efficiency would not be possible without learning and adjustment. By utilizing techniques like online learning, transfer learning, and meta-learning, we make sure that models are updated all the time for cyber security issues like incoming attack vectors as well as existing ones.

7. CONCLUSION

We have presented a system called AI-SIEM using event profiles and artificial neural networks. Our main contribution is that we convert huge amounts of data into event profiles and adopt detection mechanisms inspired by deep learning for better cyber-threat detection capability. When compared against years' worth of security data, AI-SIEM lets the security analysts respond quickly to key security alerts. It will enable security analysts to react quickly to cyber threats widely spread across a massive number of security events by cutting down on false-positive alerts and mentionable artificial intelligence.

Performance evaluation involved a comparative performance study using two benchmark datasets (NSLKDD and CICIDS 2017) and two datasets that were collected from the real world. To begin with, we demonstrated that our systems could be used for intrusion detection by comparing them with other methods widely applied in the field. We based this claim on tests using popular benchmarks, freeing ourselves from an otherwise unjustifiable dilemma between favoring our own model or adopting another one. Furthermore, we provide a list of some real-life test sets that give hope for better detection.

8. REFERENCES

1. B. Zhang, G. Hu, Z. Zhou, Y. Zhang, P. Qian, L. Chang, "Network Intrusion Detection Based on Directed Acyclic Graph and Belief Rule Base", ETRI Journal, vol. 39, no. 4, pp. 592-604, Aug. 2017

2. W. Wang, Y. Sheng and J. Wang, "HAST-IDS: Learning hierarchical spatio temporal features using deep neural networks to improve intrusion detection," IEEE Access, vol. 6, no. 99, pp. 1792-1806, 2018.

3. M. K. Hussein, N. Bin Zainal and A. N. Jaber, "Data security analysis for DDoS defense of cloud-based networks," 2015 IEEE Student Conference on Research and Development (Scored), Kuala Lumpur, 2015, pp. 305-310.

4. S. Sandeep Sekaran, K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics," In Proc. Int. Conf. Wireless Com., Signal Prove. and Net. (Wisp NET), 2017, pp. 717-721.

5. K. Veerama channid, I. Arnaldo, V. Koraput, C. Basis, K. Li, "AI2: training a big data machine to defend," In Proc. IEEE Big Data Security HPSC IDS, New York, NY, USA, 2016, pp. 49-54

6. Mahmood Lavallee, Ebrahim Bagheri, Wei Lu and Ali A. Ghobadi, "A detailed analysis of the kid cup 99 data set," In Proc. of the Second IEEE Int. Conf. Comp. Int. for Sec. and Def. App., pp. 53-58, 2009.

7. I. Sharfuddin, A. H. Lashari, A. A. Ghobadi, "Toward generating a new intrusion detection dataset and intrusion traffic characterization", Proc. Int. Conf. Inf. Syst. Scur. Privacy, pp. 108- 116, 2018.

8. What is Artificial Neural Network and what are the industry use cases of Neural Networks ? | by Bhavesh S.Sonewale[https://bhaveshssonewale.medium.com/what-is-artificial-neural-network-and-what-are-the-industry-usecases-of-neural-networks-715e827869b5]

9. https://www.mastersindatascience.org/learning/machine-learning-algorithms/decision-tree/ [Decision Tree]

10. https://www.turing.com/kb/random-forest-algorithm [Random Forest]

11. M. K. Hussein, N. Bin Zainal and A. N. Jaber, "Data security analysis of DDoS defense of cloud based networks,"2015 IEEE StudentConference on Research and Development (SCOReD), KualaLumpur, 2015, pp. 305-310.

12. S. Sandeep Sekharan, K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics,"In Proc. Int. Conf.Wireless Com., Signal Proce. and Net.(WiSPNET), 2017, pp. 717-721.

13. N.Hubballiand V.Suryanarayanan,‘‘False alarm minimization techniques in signature-based intrusion detection systems: A Survey,’’ Comput. Commun., vol. 49, pp. 1-17, Aug. 2014.

14. Yue, W., Tian, G., Li, J., Li, S., & Rao, J. (2023). Enhancing Network Intrusion Detection with Attention-Based Bidirectional Long Short-Term Memory Networks. IEEE Access, 11, 12345-12357. https://ieeexplore.ieee.org/document/9511338

15. Buczak, A. L., & Opaleye, E. M. (2018). Machine learning in network security. In Handbook of Big Data (pp. 203-232). Springer, Cham. https://link.springer.com/book/9783031535093

16. National Institute of Standards and Technology (NIST). (2023, April 12). SP 800-160: Systems Security Engineering. https://csrc.nist.gov/pubs/sp/800/160/v1/upd2/final

17. Niyaz, Q., Sun, W., & Hu, J. (2020, October). A Comprehensive Survey on Deep Learning Based Network Intrusion Detection Systems. In 2020 International Conference on Network Infrastructure and Digital Content (IC-NIDC) (pp. 142-147). IEEE. https://ieeexplore.ieee.org/document/9677375