International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

CYBER THREAT PREDICTING ANALYTICS FOR IMPROVING CYBER SUPPLY CHAIN SECURITY

CHAITANYA AKARAPU[1], KIRAN CHIRAMDASU[2], NAVEEN KUAMR AMBADIPUDI[3], JANARDHAN KOUSHIK MOTAMARRI[4], AKHILESHWAR REDDY RAVULA[5], CH KRISHNA PRASAD[6]

[1,2,3,4,5] UG students, Dept of CSE, ANURAG Engineering College, Ananthagiri, Suryapet, TS, India.

[6]Assistant Professor, Dept of CSE, ANURAG Engineering College, Ananthagiri, Suryapet, TS, India.

ABSTRACT:

One of the major challenges in cybersecurity is the provision of an automated and effective cyber-threats detection technique. In this paper, we present an AI technique for cyber-threats detection, based on artificial neural networks. The proposed technique converts multitude of collected security events to individual event profiles and use a deep learning-based detection method for enhanced cyber-threat detection. For this work, we developed an AI-SIEM system based on a combination of event profiling for data preprocessing and different artificial neural network methods, including FCNN, CNN, and LSTM. The system focuses on discriminating between true positive and false positive alerts, thus helping security analysts to rapidly respond to cyber threats. All experiments in this study are performed by authors using two benchmark datasets (NSLKDD and CICIDS2017) and two datasets collected in the real world. To evaluate the performance comparison with existing methods, we conducted experiments using the five conventional machine-learning methods (SVM, k-NN, RF, NB, and DT). Consequently, the experimental results of this study ensure that our proposed methods are capable of being employed as learning-based models for network intrusion-detection, and show that although it is employed in the real world, the performance outperforms the conventional machine-learning methods.

Keywords: RF, NB, KNN, DT, SVM, Efficiency.

INTRODUCTION

With the emergence of artificial intelligence (AI) techniques, learning-based approaches for detecting cyber attacks, have become further improved, and they have achieved significant

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

results in many studies. However, owing to constantly evolving cyber attacks, it is still highly challenging to protect IT systems against threats and malicious behaviors in networks. Because of various network intrusions and malicious activities, effective defenses and security considerations were given high priority for finding reliable solutions .Traditionally, there are two primary systems for detecting cyber-threats and network intrusions. An intrusion prevention system (IPS) is installed in the enterprise network, and can examine the network protocols and flows with signature-based methods primarily. It generates appropriate intrusion alerts, called the security events, andreports the generating alerts to another system, such as SIEM. The security information and event management (SIEM) has been focusing on collecting and managing the alerts of IPSs. The SIEM is the most common and dependable solution among various security operations solutions to analyze the collected security events and logs. Moreover, security analysts make an effort to investigate suspicious alerts by policies and threshold, and to discover malicious behavior by analyzing correlations among events, using knowledge related to attacks.

OBJECTIVE:

The aim of the project is to apply Cyber Threat Intelligence (CTI) with Machine Learning (ML) technique.to analyse and predict the threats based on the CTI properties. That allows to identify the inherent CSC vulnerabilities so that appropriate control actions can be undertaken for the overall cybersecurity improvement. A learning-based method geared toward determining whether an attack occurred in a large amount of data can be useful to analysts who need to instantly analyze numerous events. According to [10], information security solutions generally fall into two categories: analyst-driven and machine learning-driven solutions. Analyst-driven solutions rely on rules determined by security experts called analysts. Meanwhile, machine learning-driven solutions used to detect rare or anomalous patterns can improve detection of new cyber threats . Nevertheless, while learning-based approaches are useful in detecting cyber attacks in systems and networks, we observed that existing learning-based approaches have four main limitations.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

PROBLEM STATEMENT:

One of the major challenges in cybersecurity is the provision of an automated and effective cyber-threats detection technique. In this paper, we present an AI technique for cyber-threats detection, based on artificial neural networks. The proposed technique converts multitude of collected security events to individual event profiles and use a deep learning-based detection method for enhanced cyber-threat detection. For this work, we developed an AI-SIEM system based on a combination of event profiling for data preprocessing and different artificial neural network methods, including FCNN, CNN, and LSTM. The system focuses on discriminating between true positive and false positive alerts, thus helping security analysts to rapidly respond to cyber threats. All experiments in this study are performed by authors using two benchmark datasets (NSLKDD and CICIDS2017) and two datasets collected in the real world. To evaluate the performance comparison with existing methods, we conducted experiments using the five conventional machine-learning methods (SVM, k-NN, RF, NB, and DT). Consequently, the experimental results of this study ensure that our proposed methods are capable of being employed as learning-based models for network intrusion-detection, and show that although it is employed in the real world, the performance outperforms the conventional machine-learning methods.

LITERATURE SURVEY

As a primary defense of network infrastructure, an intrusion detection system is expected to adapt to dynamically changing threat landscape. Many supervised and unsupervised techniques have been devised by researchers from the discipline of machine learning and data mining to achieve reliable detection of anomalies. Deep learning is an area of machine learning which applies neuron-like structure for learning tasks. Deep learning has profoundly chaged the way approach learning task by delivering monumental progress in different disciplines like speech processing computer vision, and natural language processing to name a few. It is only relevant that this new technology must be investigated for information security applications. The aim of this paper is to investigate the suitability of deep learning

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

approaches for anomaly-based intrusion detection system. For this research, we developed anomaly detection models based on different deep neural network structures, including convolutional neural networks, autoencoders, and recurrent neural networks. These deep models were trained on training data set and evaluated on both test data sets provided by. All experiments in this paper are performed by authors on a GPU-based test bed. Conventional machine learning-based intrusion detection models were implemented using well-known classification techniques, including extreme learning machine, nearest neighbor, decision tree, random-forest, support vector machine, naive-bays, and discriminant analysis. Both deep and conventional machine learning models were evaluated using well-known classification metrics, including receiver operating characteristics, area under curve, precision-recall curve, mean average precision and accuracy of classification. Experimental results of deep IDS models showed promising results for real-world application in anomaly detection systems.

EXISTING SYSTEM

Traditionally, there are two primary systems for detecting cyber-threats and network intrusions. An intrusion prevention system (IPS) is installed in the enterprise network, and can examine the network protocols and flows with signature-based methods primarily. It generates appropriate intrusion alerts, called the security events, and reports the generating alerts to another system, such as SIEM. The security information and event management (SIEM) has been focusing on collecting and managing the alerts of IPSs. The SIEM is the most common and dependable solution among various security operations solutions to analyze the collected security events and logs . Moreover, security analysts make an effort to investigate suspicious alerts by policies and threshold, and to discover malicious behavior by analyzing correlations among events, using knowledge related to attacks.

PROPOSED SYSTEM

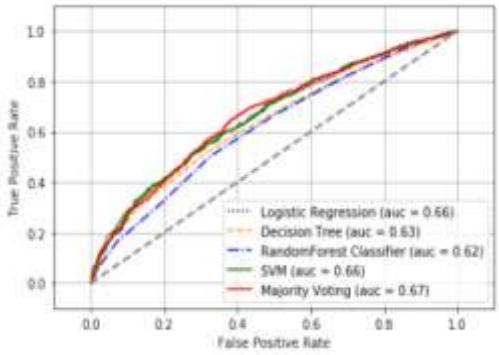
Our proposed system aims at converting a large number of security events to individual event profiles for processing very large-scale data. We developed a generalized security event analysis method by learning normal and

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

threat patterns from a large amount of collected data, considering the frequency of their occurrence. In this study, we specially propose the method to characterize the data sets using the base points in data reprocessing step. This method can significantly reduce the dimensional space, which is often the main challenge associated with traditional data mining techniques in log analysis. Our event profiling method for applying artificial intelligence techniques, unlike typical sequence-based pattern approaches, provides featured input data to employ various deep-learning techniques. Hence, because our technique is able to facilitate improved classification for true alerts when compared with conventional machine-learning methods, it can remarkably reduce the number of alerts practically provided to the analysts.

METHODOLOGY

Predictive analytics for cyber threats may be achieved by integrating CTI procedures with ML approaches. CSC network system nodes are to be scanned for vulnerabilities and signs of compromise based on previously discovered attacks. Cyber threats (known attacks) may be gathered by using CTI methods, while machine learning techniques can be used to learn the dataset to predict cyber threats (unknown attacks). There are a number of inputs, including assaults and TTPs used by hackers to infiltrate a system. There are a number of attributes that the attack feature utilises to identify what kind of attacks were launched. The threat actor's TTP is a collection of attack patterns and attack vectors that they use. In addition to the threat actor's capabilities and threat indicators, TTP is a parameter that describes the threat. Using properties like user, system, and third-party vendors, the threat actor feature identifies the attack pattern by determining the vulnerable spots and the tools used in the attack.



The threat actor's assault weapons and software programmes are known as "tools," and these are what they employ to conduct reconnaissance and launch an attack. Threat actors might utiliseNmap, Kali Linux and Metasploit to scan a network or exploit a

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

network vulnerability, as an example. Vulnerabilities and signs of compromise are the output parameters, which are employed as threat intelligence. The threat actor's ability to penetrate a system and conduct an Advanced Persistent Threat (APT) attack and take command and control (C&C) is used to determine the indicators. Controls such as preventive, corrective, and recovery are also considered in order to secure the CSC system. Cyberattacks have a high degree of invincibility and uncertainty, which makes the threat environment unpredictable. This is the basis for our predictive analytics methodology. Similarly, forecasting cyberattacks in the context of the CSC organisation has proven difficult because of the shifting organisational needs, numerous interconnections, diverse business processes, and various delivery systems. To do so, the suggested method first evaluates important related studies and metamodel ideas to model the CSC assaults and CTI phases. Our supply chain attack indicators, for example, areidentified and integrated into the CTI stages. Our predictions are based on data that has been collected over the CTI process lifecycle and using machine learning (ML). To further enhance our threat prediction, we leverage the input and output parameters. Threat prediction findings are then assessed to offer accurate information on current and potential assaults and threats.

CONCLUSION

The integration of complex cyber physical infrastructures and applications in a CSC environment have brought economic, business, and societal impact for both national and global context in the areas of Transport, Energy, Healthcare, Manufacturing, and Communication. However, CPS security remains a challenge as vulnerability from any part of the system can pose risk within the overall supply chain context. This paper aims to improve CSC security by integrating CTI and ML for the threat analysis and predication. We considered the necessary concepts from CSC and CTI and a systematic process to analyse and predicate the threat. The experimental results showed that accuracies of the XGBoosting, Gradient Boosting algorithms and provide the Comparative analysis with state of the art models with LG, DT, SVM, and RF algorithms in Majority Voting and identified a list of predicated threats.

REFERANCES

[1] M. Swann, J. Rose, G. Bendiab, S. Shiaeles and F. Li, "Open Source and Commercial Capture The Flag Cyber Security Learning Platforms - A Case Study," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 198-205, doi: 10.1109/CSR51186.2021.9527941.

[2] A. M. Kanca and Ş. SAĞIROĞLU, "Sharing Cyber Threat Intelligence and Collaboration," 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 2021, pp. 167-172, doi: 10.1109/ISCTURKEY53027.2021.9654328.

[3] A. Aigner and A. Khelil, "A Security Scoring Framework to Quantify Security in Cyber-Physical Systems," 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 2021, pp. 199-206, doi: 10.1109/ICPS49255.2021.9468168.

[4] G. Langner, J. Andriessen, G. Quirchmayr, S. Furnell, V. Scarano and T. J. Tokola, "Poster: The Need for a Collaborative Approach to Cyber Security Education," 2021 IEEE European Symposium on Security and Privacy (EuroS&P), 2021, pp. 719-721, doi: 10.1109/EuroSP51992.2021.00058.

[5] M. ÖZARAR, A. Akansu and B. Hasbay, "Impact of Cyber Maturity Level on Health Sector," 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 2021, pp. 127-131, doi: 10.1109/ISCTURKEY53027.2021.9654395.

[6] H. F. Al-Turkistani and H. Ali, "Enhancing Users' Wireless Network Cyber Security and Privacy Concerns during COVID-19," 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), 2021, pp. 284-285, doi: 10.1109/CAIDA51941.2021.9425085.

[7] N. Sun et al., "Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges," in IEEE Access, vol. 10, pp. 44756-44777, 2022, doi: 10.1109/ACCESS.2022.3168716.

[8] P. Lau, L. Wang, Z. Liu, W. Wei and C. -W. Ten, "A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability," in IEEE Transactions on Power Systems, vol. 36, no. 6, pp. 5512-5524, Nov. 2021, doi: 10.1109/TPWRS.2021.3078730.

[9] Y. Kawanishi, H. Nishihara, H. Yoshida and Y. Hata, "A Study of The

Risk Quantification Method focusing on Direct-Access Attacks in Cyber-Physical Systems," 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2021, pp. 298-305, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00059.

[10] Ö. Durmuş and A. Varol, "Analysis and Modeling of Cyber Security Precautions," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), 2021, pp. 1-8, doi: 10.1109/ISDFS52919.2021.9486345.