ISSN: 2278-4632
Vol-13, Issue-04, No.06, April : 2023

CYBER ENCROACHMENT DETECTION BASED ON INTELLIGENT RETRIEVAL NETWORKS USING EVENT PROFILES

Chitla.Vinay Santhosh[1], [1]Assistant Professor, Department of Computer Science and Engineering
DVR & Dr. HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India
D.Varun Prasad[2],[2]Associate Professor, Department of Computer Science and Engineering
DVR & Dr. HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India
Sravani Kilari[3], Satish Bathula[4], Rajesh Jagathi[5], Sravana Sandhya Meesala[6]
[3,4,5,6]UG Student, Department of Computer Science and Engineering
DVR & Dr. HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India

Abstract:

One of the significant difficulties in network protection is the arrangement of a robotized and compelling digital dangers discovery method. In this paper, we present a simulated intelligence procedure for digital dangers discovery, in view of fake brain organizations. The proposed procedure changes large number ofgathered security occasions over completely to individual occasion profiles and utilize a profound learning-based location technique for upgraded digital danger discovery. For this work, we fostered a simulated intelligence SIEM framework in light of a mix of occasion profiling for information preprocessingand different counterfeit brain network techniques, including FCNN, CNN, and LSTM.

The frame work centers around segregating between evident positive and misleading positive alarms, consequentlyhelping security investigators to quickly answer digital dangers. All analyses in thisstudy are performed by creators utilizing two benchmark datasets (NSLKDD and CICIDS2017) and two datasets gathered in reality. To assess the exhibition examination with existing strategies, we led tests utilizing the five customary AI techniques (SVM, k-NN, RF, NB, and DT). Subsequently, the exploratory consequences of this study guarantee that our proposed strategies are fit for being utilized as learning-based models for network interruption discovery, and show that in spite of the fact that it is utilized in reality the execution bears the ordinary AI techniques.

1. Introduction:

Learning-based systems for identifying cyber assaults have developed further with the development of artificial intelligence (AI) capabilities, and they have shown considerable outcomes in numerous studies. Yet, protecting IT systems from threats and criminal network behaviour is still very difficult because cyber attacks are always changing. Effective defences and security concerns were given significant priority for establishing dependable solutions because of numerous network intrusions and malicious actions [1], [2], [3], [4].

For identifying network intrusions and cyber threats, there are typically two main systems. The company network has an intrusion prevention system (IPS) installed, which uses signature-based techniques to primarily inspect network protocols and flows. It produces the necessary intrusion alerts, also known as security events, and reports the alert generation to another system, like SIEM. The gathering and administration of IPS detect [6], [7]. Hence, machine learning and artificial intelligence algorithms for identifying attacks have received moreattention in the most recent studies in the field of intrusion detection. The development of AI-related domains can help security experts investigate network

For analysts who need to quickly determine a huge number of events, a learning-based approach targeted towards evaluating whether an attack occurred in a big amount of data can be helpful. [10] states that information security solutions often fall into two categories: those driven by analysts and alerts has been the primary focus of security information and event management (SIEM). The SIEM is the most common and dependable option among several security operations solutions to analyse the gathered security events and logs [5]. Moreover, security analysts work to evaluate suspicious alerts based on policies and thresholds and to find malicious behaviour by looking at

 DOI: 10.36893.JK.2023.V13I04N16.00245-00250

correlations between events and applying attack-related knowledge. Because to their high false alarm rates and the huge volume of security data, intrusions against intelligent network attacks are still challenging to distinguish and attacks quickly and automatically. The attack model must be learned from previous threat data for these learning- based approaches, and trained models must be used to find intrusions for unidentified cyber threats [8], [9]. those powered by machine learning. Analyst-driven solutions rely on guidelines created by analysts, or security specialists. Meanwhile, systems powered by machine learning that look for uncommon or unusual patterns can help identify future cyberthreats better [10]. We found that existing learning-based techniques have four fundamental drawbacks, despite the fact that they are useful for identifying cyber attacks in systems and networks.Firstly, labelled data are necessary for Third, while utilising an anomaly-based approach to identify network intrusion might assist identify unidentified cyber threats, it can also result in a high proportion of false alarms [6]. It is quite expensive to set off numerous false positive alerts, and it takes a considerable amount of work from staff to investigate them. Fourth, some hackers can slowly alter their behavioural patterns to conceal their malicious operations [10],[14]. The detection models are inadequate because attackers frequently alter their behaviour, even when proper learning- based models are possible. Also, the majority of security systems have been concentrated on the analysis of recent network security incidents. We think that, over long periods of time, examining the security event history connected with the origination of events can be one method of identifying the malicious actors behind continually evolving attacks.learning-based detection techniques since they allow for model training and evaluation. Additionally, obtaining such labelled data at a scale that enables precise odel training is difficult. Several current SIEM solutions do not keep labelled data that can be used with supervised learning models, despite the requirement for labelled data[10].Second, because they are not included in widespread network security systems, the majority of the learning features that are theoretically employed in each study are not generic features in the real world [3]. As a result, it is challenging to apply to real- world situations. Deep learning technologies have been considered in recent intrusion detection research efforts, and performance has been assessed using well-known datasets including NSLKDD [11], CICIDS2017 [12], and Kyoto-Honeypot [13]. Nevertheless, a lot of earlier studies used benchmark datasets that, while accurate, could not be applied to thereal world due to a lack of characteristics. An applied learning model must be evaluated using real- world datasets in order to get over these constraints.These challenges form the primary motivation for this work. To address these challenges, we present an AI-SIEM system which is able to discriminate between true alerts and false alerts based on deep learning techniques.

Our proposed system can help security analysts rapidly to respond cyber threats, dispersed across a large amount of security events. For this, the proposed the AI-SIEM system particularly includes an event pattern extraction method by aggregating together events with a concurrency feature and correlating between events sets in collected data. Our event profiles have the potential to provide concise input data for various deep neural networks. Moreover, itenables the analyst to handle all the data promptly and efficiently by comparison with long-term history data.

2. RELATED WORK:

Enhanced Network Anomaly DetectionBased on Deep Neural Networks :

Due to the monumental growth of Internet applications in the last decade, the need for security of information network has increased manifolds. 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 changed the way we approach learning tasks 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

 DOI: 10.36893.JK.2023.V13I04N16.00245-00250

applications. The aim of this paper is to investigate the suitability of deep learning 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 NSLKDD training data set and evaluated on both test data sets provided by NSLKDD, namely NSLKDDTest+ and NSLKDDTest21. 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 quadratic 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.

Network Intrusion Detection Based on Directed Acyclic Graphand Belief Rule Base

Intrusion detection is very important for network situation awareness. While a few methods have been proposed to detect network intrusion, they cannot directly and effectively utilize semi-quantitative information consisting of expert knowledge and quantitative data. Hence, this paper proposes a new detection model based on a directed acyclic graph (DAG) and a belief rule base (BRB). In the proposed model, called DAG-BRB, the DAG is employed to construct a multi-layered BRB model that can avoid explosion of combinations of rule number because of a large number of types of intrusion. To obtain the optimal parameters of the DAG-BRB model, an improved constraint covariance matrix adaption evolution strategy (CMA-ES) is developed that can effectively solve the constraint problem in the BRB. A case study was used to test the efficiency of the proposed DAG-BRB. The results showed that compared with other detection models, the DAG-BRB model has a higher detection rate and can be used in real networks.

HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection

The development of an anomaly-based intrusion detection system (IDS) is a primary research direction in the field of intrusion detection. An IDS learns normal and anomalous behavior by analyzing network traffic and can detect unknown and new attacks. However, the performance of IDS is highly dependent on feature design, and designing a feature set that can accurately characterize network traffic is still an ongoing research issue. Anomaly-based IDSs also have the problem of a high false alarm rate (FAR), which seriously restricts their practical applications. In this paper, we propose a novel IDS called the hierarchical spatial- temporal features-based intrusion detection system (HAST-IDS), which first learns the low-level spatial features of network traffic using deep convolutional neural networks (CNNs) and then learns high- level temporal features using long short- term memory networks. The entire process of feature learning is completed by the deep neural networks automatically; no feature engineering techniques are required. The automatically learned traffic features effectively reduce the FAR. The standard DARPA1998 and ISCX2012 datasets are used to evaluate the performance of the proposed system. The experimental results show that the HAST-IDS outperforms other published approaches in terms of accuracy, detection rate, and FAR, which successfully demonstrates its effectiveness in both feature learning and FAR reduction.

Data security analysis for DDoSdefense of cloud based networks

Distributed computing has become an effective approach to enhance capabilities of an institution or organization and minimize requirements for additional resource. In this regard, the distributed computing helps in broadening institutes IT capabilities. One needs to note that distributed computing is now integral part of most expanding IT business sector. It is considered novel and efficient means for expanding business. As more organizations and individuals start to use the cloud to store their data and applications, significant concerns have developed to protect sensitive data

ISSN: 2278-4632
Vol-13, Issue-04, No.06, April : 2023

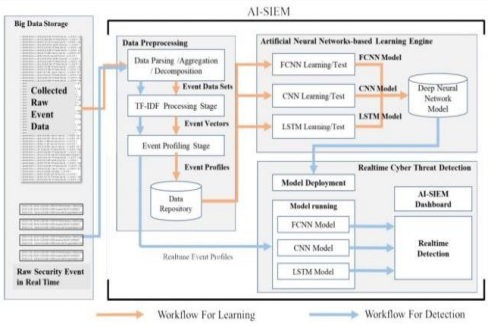
from external and internal attacks over internet. Due to security concern many clients hesitate in relocating their sensitive data on the clouds, despite significant interest in cloud-based computing. Security is a significant issue, since data much of anorganizations data provides a tempting target for hackers and those concerns will continue to diminish the development of distributed computing if not addressed. Therefore, this study presents a new test and insight into a honeypot. It is a device that can be classified into two types: handling and research honeypots.Handling honeypots are used to mitigate real life dangers. A research honeypot is utilized as an exploration instrument to study and distinguish the dangers on the internet. Therefore, the primary aim of thisresearch project is to do an intensive network security analysis through avirtualized honeypot for cloud servers to tempt an attacker and provide a new meansof monitoring their behavior

SYSTEM ARCHITECTURE:

The workflow and architecture for the developed artificial intelligent (AI)-based SIEM system. The AI-SIEM system comprises three main phases: The data pre-processing, artificial neural networks- based learning engine, and real-time threat detection phase. The first preprocessing phase in the system, termed event profiling, aims at providing concise inputs for various deep neural networks by transforming raw data. In the datapreprocessing phase, data aggregation with parsing, data normalization stage using TF-IDF mechanism, and event profiling stage are consecutively performed in the AI-SIEM system. Each stage generates event data sets, event vectors, and event profiles, respectively, and the output is utilized in next each stage, as shown inFigure. This phase not only precedes the data learning stage but also precedes the conversion of raw security events to the deep-learning engine's input data when the system operates on detecting network intrusions in real time. The second based learning engine employs three artificial neural networks for modeling. For the datalearning stage, the preprocessed data are

EXISTING SYSTEM:

For identifying network breaches and cyber threats, there are typically two main systems. The company network has an intrusion prevention system[IPS] installed
,which uses signature-basic techniques to primarily inspect network protocols and flows.It produces the necessary intrusion alarms , also known as security events, and reports the alerts to another system like SIEM.The gathering and administration of IPS alerts has been the primary focus of security information and event management(SIEM).Among the numerous security operations solutions,the SIEM is the most popular and dependable option for analysing the gathered security events and logs. Moreover, security analysts work to examine suspicious alerts based on fed into the three artificial neural networks, and each ANN performs learning to find the most accurate model. Finally, in real-time threat detection, each ANN model mechanically classifies each security raw event using the trained model,and the dashboard shows the onlyrecognized true alerts to security analysts for reducing false ones.



policies and thresholds and to find malicious behaviour by examining correlations between events and applying attack-related knowledge

DOI: 10.36893.JK.2023.V13I04N16.00245-00250

ISSN: 2278-4632
Vol-13, Issue-04, No.06, April : 2023

3. PROPOSED SYSTEM:

By grouping events with a concurrency feature and comparing event sets in thecollected data, the proposed AI-SIEM system includes an event pattern extraction method in particular. Our event profiles have the potential to provide concise input data for various deep neural networks. Additionally it gives the analyst the ability to quickly and effectively manage all the data through comparison with long termhistory data.

4. RESULT ANALYSIS:

In above graph x-axis represents algorithm name and y-axis represents accuracy of those algorithms and from above graph we can conclude that LSTM and CNN perform well. Now click on Precision Comparison Graph to get below graph.

5. CONCLUSION:

In this paper, we have proposed the AI- SIEM system using event profiles and artificial neural networks. The novelty of our work lies in condensing very large-scale data into event profiles and using the deep learning-based detection methods for enhanced cyber-threat detection ability.The AI-SIEM system enables the security analysts to deal with significant security alerts promptly and efficiently by comparing long-term security data. By reducing false positive alerts, it can also help the security analysts to rapidly respond to cyber threats dispersed across a large number of security events.

REFERENCES

[1]S. Naseer, Y. Saleem, S. Khalid, M. K.Bashir, J. Han, M. M. Iqbal,K. Han, "Enhanced Network Anomaly Detection Based on DeepNeural Networks," IEEE Access, vol. 6, pp. 48231-48246, 2018.

[2]B. Zhang, G. Hu, Z. Zhou, Y. Zhang,

[3]P. Qiao, L. Chang, "NetworkIntrusion Detection Based on Directed Acyclic Graph and Belief RuleBase", ETRI Journal, vol. 39, no. 4, pp. 592-604, Aug.2017

[4]W. Wang, Y. Sheng and J. Wang, "HAST-IDS: Learning hierarchicalspatial-temporal features using deep neural networks to improveintrusion detection," IEEE Access, vol. 6, no. 99, pp. 1792- 1806,2018.

[5]M. K. Hussein, N. Bin Zainal and A.

[6]N. Jaber, "Data security analysisfor DDoS defense of cloud based networks," 2015 IEEE StudentConference on Research andDevelopment (Scored), KualaLumpur, 2015, pp. 305-310.

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

[8]N.Hubballiand V.Surya Narayanan

[9],‘‘False alarm minimizationtechniques insignature-based intrusion detection systems: Asurvey,’’ Comput. Commun., vol. 49, pp. 1-17, Aug. 2014.

[10] A. Naser, M. A. Majid, M. F. Zolkipli and S. Anwar, "Trusting cloudcomputing for personal files," 2014 International Conference onInformation and Communication Technology Convergence(ICTC),Busan, 2014, pp. 488-489.

[11] Y. Shen, E. Mariconti, P. Vervier, andGianluca Stringhini, "Tiresias:Predicting Security Events

 DOI: 10.36893.JK.2023.V13I04N16.00245-00250

ISSN: 2278-4632
Vol-13, Issue-04, No.06, April : 2023

Through Deep Learning,"In Proc. ACMCCS 18, Toronto, Canada, 2018, pp. 592-605.
[12] Kyle Soska and Nicolas Christin, "Automatically detectingvulnerable websites before they turn malicious,", In Proc. USENIXSecurity Symposium., SanDiego, CA, USA, 2014, pp.625-640.
[13] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, K. Li,"AI2: training a big data machine to defend," In Proc. IEEEBigDataSecurity HPSC IDS, New York, NY, USA, 2016, pp. 49-54
[14] Mahbod Tavallaee, Ebrahim Bagheri,Wei Lu and Ali A. Ghorbani,"A detailed analysis of the kdd cup 99 data set," In Proc. of theSecond IEEE Int. Conf. Comp.Int. for Sec. and Def. App., pp. 53-58,
[15] 2009.
[16] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, "Toward generatinga new intrusion detection dataset and intrusion traffic characterization", Proc. Int. Conf.
Inf. Syst. Secure. Privacy, pp. 108-116,2018.
[1] [online] Available: http://www.takakura.com/Kyoto_data/
[2] N. Shone, T. N. Ngoc, V. D. Phai and
Q. Shi, "A deep learningapproach to network intrusion detection," IEEE Trans. Emerg. TopicsComput. Intell., vol. 2, pp. 41-50, Feb. 2018
[3] R. Vinayakumar, Mamoun Alazab, K.
P. Soman, P. Poornachandran,Ameer Al-Nemrat and Sitalakshmi Venkatraman, "Deep LearningApproach for Intelligent Intrusion Detection System," IEEE Access,vol. 7, pp. 41525-41550, Apr. 2019.

 DOI: 10.36893.JK.2023.V13I04N16.00245-00250