IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S03):75-78, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0319
Available online at: https://www.ijmtst.com/vol8si03.html

Cyber Threat Detection Based on Artificial Neural Networks using Event Profiles

K. Suryakala | CH. Sujitha | N. Nikhil Sai Raj | D. Surendra Kumar | A.N.V.B Sai Kiran

Department of Computer Ccience and Engineering, Godavari Institute of Engineering and Technology(A), JNTUK, Kakinada.

To Cite this Article

K. Suryakala, CH. Sujitha, N. Nikhil Sai Raj, D. Surendra Kumar and A.N.V.B Sai Kiran. Cyber Threat Detection Based on Artificial Neural Networks using Event Profiles. International Journal for Modern Trends in Science and Technology 2022, 8(S03), pp. 75-78.https://doi.org/10.46501/IJMTST08S0319

Article Info

Received: 26 April 2022; Accepted: 24 May 2022; Published: 30 May 2022.

ABSTRACT

One of the most fundamental issues in cybersecurity is the provision of a computerized and advantageous cyber-threat detection strategy. We present a synthetic neural network-based AI technique for detecting cyber-threats in this paper. The proposed method converts a large number of accumulated safety events into man or woman match profiles and employs a deep learning-based detection approach for more effective cyber-threat identification. We built an AI-SIEM system for this project using a combination of match profiling for data preprocessing and novel synthetic neural community approaches like FCNN, CNN, and LSTM

1.INTRODUCTION

Learning based approaches to detecting cyber attacks have been improved with the advent of artificial intelligence (AI) techniques, with significant results in many studies. However, due to the ever-changing nature of cyber attacks, it is still very difficult to protect IT systems from threats and malicious network behavior. In order to find dependable solutions, effective defenses and security considerations were prioritized due to a variety of network intrusions and malicious activities. To detect cyber-threats and network intrusions, two primary systems have traditionally been used. It results in the necessary intrusion. Chi-Yuan Chen was the associate editor in charge of coordinating the review and approval of this manuscript for publication. alerts, also known as security events, and forwards them to another system, such as SIEM. Traditionally, SIEM has been used to collect and manage IPS alerts. Among various security operations solutions, the SIEM is the most common and dependable solution for analyzing collected security events and logs. In addition, security analysts investigate suspicious alerts based on policies and thresholds, as well as detect malicious behavior by analyzing correlations between events and applying attack knowledge. Despite this, it remains difficult to recognize and detect intrusions against intelligent network attacks due to the high number of false alerts and the massive amount of security data. As a result, recent intrusion detection research has placed a premium on machine learning and artificial intelligence techniques for detecting attacks. Artificial intelligence advancements can help security analysts investigate network intrusions in a timely and automated manner. [16]These learning-based approaches necessitate constructing the attack model from historical threat data and then employing the trained models to detect intrusions from unknown cyber threats.[17] A learning-based method for determining whether an attack occurred in a large amount of data can be useful for analysts who need to analyse numerous events in real time. According to, there

are two types of information security solutions: analyst-driven solutions and machine learning-driven solutions. Analyst-driven solutions are based on rules established by security analysts. Meanwhile, machine learning-driven solutions for detecting unusual or unusual patterns can aid in the detection of new cyber threats. Despite the fact that learning-based approaches are useful for detecting cyber attacks in systems and networks, we discovered 4 major limitations in existing learning-based approaches.To begin, in learning-based detection methods, labelled data is required for model training and evaluation of generated learning models. It's also difficult to collect such labelled data on a large enough scale to allow for accurate model training. Despite the need for labelled data, many commercial SIEM solutions do not keep labelled data that can be used in supervised learning models. because most common network security systems do not include the majority of The learning characteristics that are theoretically used in each study are not generalizable in the real world. As a result, it is difficult to apply to real-world situations. Recent An automation approach based on deep learning technologies has been considered in intrusion detection research efforts, with performance measured using well-known datasets such as NSLKDD, CICIDS2017, and Kyoto-Honeypot.

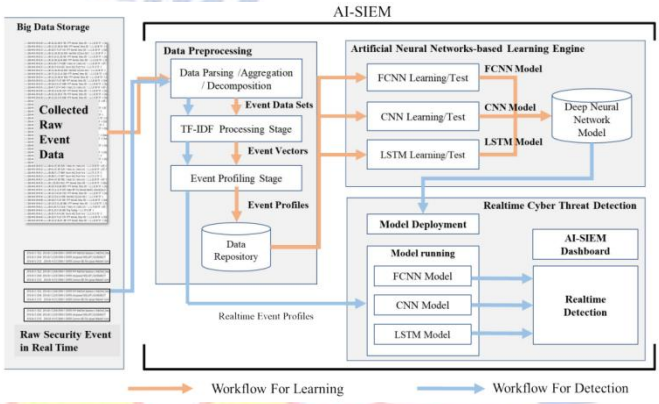
2. EXISTING SYSTEM

Despite the truth that gaining knowledge of-primarily based totally strategies are powerful in detecting cyber attacks in structures and networks, we determined 4 primary drawbacks. To begin, gaining knowledge of-primarily based totally detection strategies necessitate labelled statistics to permit for version schooling and evaluation. Furthermore, acquiring such labelled statistics at a scale that lets in for correct version schooling is difficult. Despite the significance of labelled statistics, many industrial SIEM answers do now no longer hold labelled statistics that may be used with supervised gaining knowledge of models. Second, due to the fact they may be now no longer covered in traditional community safety structures, maximum of the gaining knowledge of functions which are theoretically hired in every have a look at aren't generalized functions with inside the actual world. As a result, it's miles difficult to use.

3.PROPOSED SYSTEM

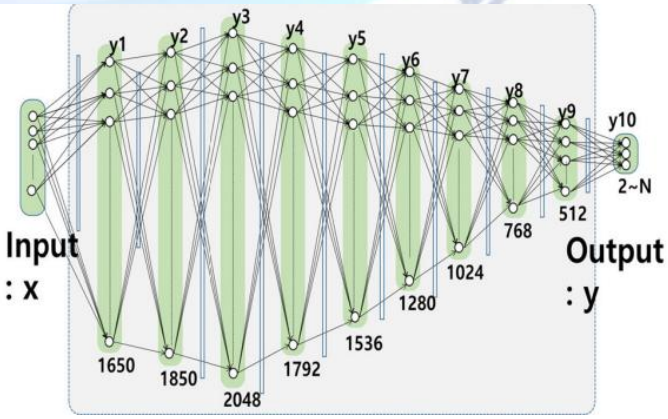
In this paper author is describing concept to detect threats using AI-SIEM technique which is a combination of deep learning algorithms like FCNN, CNN and LSTM and this technique works based on events profiling such as attack signatures. Author evaluating propose work performance with conventional techniques. Here I am implementing CNN and LSTM algorithms.

AI-SIEM



FCNN

FCNN is the most popular deep learning network where all the nodes in the fully connected layer are connected to all the nodes in the layer below. Each node in the FCNN is connected to all nodes in the previous layer, and each connection has a unique weight that is not shared by all nodes. FCNNs are simpler than traditional CNNs and RNNs, but it was previously recognized that the zero-gradient problem during backward propagation was the cause of the inaccuracy. On the other hand, the invention of the RELU (Rectified Linear Unit) activation function solved the back propagation problem that hindered the development of artificial neural networks



CNN

CNNs are neural community topologies designed specially for coping with spatial records. The enter layer records for CNN is a 2D or three-D array, along with the

pixel cost of a picture. CNN`s middle layers are convolutional layers (Conv) and max pooling layers. A Conv layer takes a unmarried enter and convolves it with filters to create a non-stop circulate of records that may be handed directly to next layers. A Conv layer`s filters examine the overall inputted records through cutting it and extract the important thing capabilities. Calculating the scalar made of the enter bite and every clear out additionally contributes to convolution. Each clear out out`s retrieved capabilities are blended into a brand new characteristic set referred to as the characteristic set.

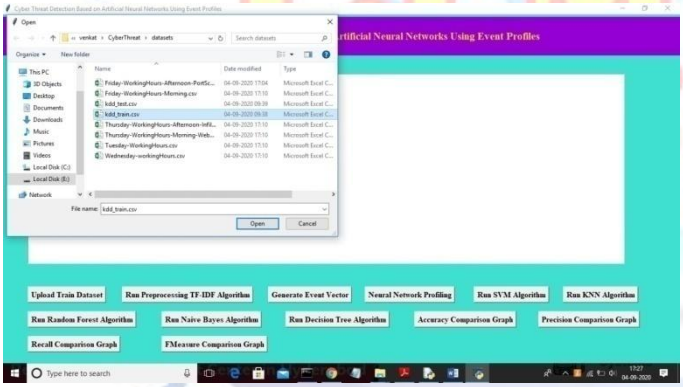
LSTM

LSTMs feature a cyclic architecture that increases storage capacity. The updated network of RNNs is called an LSTM. Unlike standard RNNs, LSTMs use dedicated memory cells to store information from previous time steps, overcoming long-term dependency issues.

4. RESULTS

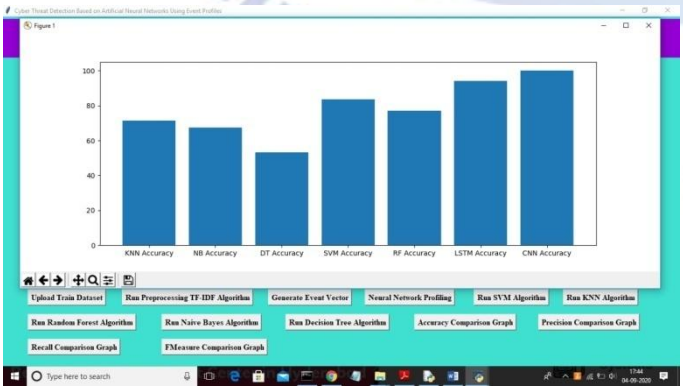
OUTPUT SCREENSHOTS

UPLOAD TRAIN DATASET



To upload a dataset as input, click on "Upload Train Dataset".

ACCURACY COMPARISON GRAPH



The x-axis in the above graph represents the algorithm name, while the y-axis represents the accuracy of those algorithms, and we can see from the graph that LSTM and CNN perform well.

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. For the evaluation of performance, we performed a performance comparison using two benchmark datasets (NSLKDD, CICIDS2017) and two datasets collected in the real world. First, based on the comparison experiment with other methods, using widely known benchmark datasets, we showed that our mechanisms can be applied as one of the learning-based models for network intrusion detection. Second, through the evaluation using two real datasets, we presented promising results that our technology also outperformed conventional machine learning methods in terms of accurate classifications. In the future, to address the evolving problem of cyber attacks, we will focus on enhancing earlier threat predictions through the multiple deep learning approach to discovering the long-term patterns in history data

Conflict of interest statement

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

REFERENCES

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, ''Enhanced network anomaly detection based on deep neural networks,'' IEEE Access, vol. 6, pp. 48231–48246, 2018.

[2] B.-C. Zhang, G.-Y.Hu, Z.-J.Zhou, Y.-M.Zhang, P.-L.Qiao, and L.-L. Chang, ''Network intrusion detection based on directed acyclic graph and belief rule base,'' Electron. Telecommun. Res. Inst. J., vol. 39, no. 4, pp. 592–604, Aug. 2017.

[3] W. Wang, Y. Sheng, and J. Wang, ''HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,'' IEEE Access, vol. 6, pp. 1792–1806, 2018.

[4] M. K. Hussein, N. Bin Zainal, and A. N. Jaber, ''Data security analysis for DDoS defense of cloud based networks,'' in Proc. IEEE

Student Conf. Res. Develop. (SCOReD), Kuala Lumpur, Malaysia, Dec. 2015, pp. 305–310.

[5] S. S. Sekharan and K. Kandasamy, ''Profiling SIEM tools and correlation engines for security analytics,'' in Proc. Int. Conf. Wireless Commun., Signal Process.Netw. (WiSPNET), Mar. 2017, pp. 717–721.

[6] N. Hubballi and V. Suryanarayanan, ''False alarm minimization techniques in signature-based intrusion detection systems: A survey,'' Comput. Commun., vol. 49, p. 1Â17, Aug. 2014.

[7] A. Naser, M. A. Majid, M. F. Zolkipli, and S. Anwar, ''Trusting cloud computing for personal files,'' in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Busan, South Korea, Oct. 2014, pp. 488–489.

[8] Y.SHEN, E. MARICONTI, P. A. VERVIER, AND G. STRINGHINI, ''TIRESIAS: PREDICTING SECURITY EVENTS THROUGH DEEP LEARNING,'' IN PROC. ACM CCS, TORONTO, ON, CANADA, OCT. 2018, PP. 592–605.

[9] K. Soska and N. Christin, ''Automatically detecting vulnerable Websites before they turn malicious,'' in Proc. USENIX Secur. Symp., San Diego, CA, USA, 2014, pp. 625–640.

[10] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, ''AI2 : Training a big data machine to defend,'' in Proc. IEEE bigdatasecurity HPSC IDS, New York, NY, USA, Apr. 2016, pp. 49–54.

[11] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, ''A detailed analysis of the KDD cup 99 data set,'' in Proc. 2nd IEEE Symp.Comput.Intell.Secur.Defense Appl., Jul. 2009, pp. 53–58.

[12] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, ''Toward generating a new intrusion detection dataset and intrusion traffic characterization,'' in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), Jan. 2018, pp. 108–116.

[13] J. Song, H. Takakura, and Y. Okabe.(2006). Description of Kyoto University Benchmark Data.[Online]. Available: http://www. Takakura.com/Kyoto_data/benchmarkdata-Description-v5.pdf

[14] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ''A deep learning approach to network intrusion detection,'' IEEE Trans. Emerg.TopicsComput.Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[15] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ''Deep learning approach for intelligent intrusion detection system,'' IEEE Access, vol. 7, pp. 41525–41550, 2019

[16] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[17] Kumar, J. R., Sujatha, B., &Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing.”