iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: https://doi.org/10.22214/ijraset.2023.56193

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

Cyber Threat Detection Based on Artificial Neural Networks

P Ramya Sai[1], K. S Niraja[2]
Department of Information Technology, BVRIT HYDERABAD College of Engineering for Women

Abstract: ***Finding an automated method for detecting cyber-attacks is one of the biggest problems in cybersecurity. We describe an artificial intelligence (AI) method based on deep learning for detecting cyber threats. The suggested solution uses a deep attempting to learn monitoring method to improve cyber-threat identification by breaking down a large volume of recorded security events into event profiles. We created an AI-SIEM system that combines event profiles for data pretreatment with several multilayer perceptron techniques, such as FCNN, CNN, and LSTM. The approach focuses on separating real positive warnings from misdiagnosis alerts to assist experts in quickly responding to cyber-attacks. We carried out tests utilising the five traditional machine-learning techniques to assess the comparison study with existing approaches (SVM, k-NN, RF, NB, and DT). The experimental findings of this study confirm that our suggested methods may be used as studying models for activity recognition and demonstrate that, when used in the real life, they outperform traditional auto techniques.***
Keywords: ANN, CNN, K-NN, LSTM, SVM

I. INTRODUCTION

The newly developed artificial intelligence (AI) tools, attempting to learn methods for identifying hacks, have produced notable outcomes. Protecting IT infrastructure from attacks and criminal network activity is still very difficult, though, because attackers are continually developing.

Strong defences and security concerns were given top importance for creating dependable remedies due to numerous network invasions and illicit behaviour. Are there normally two basic technologies for detecting network disruptions and intrusions a security system (IPS) has been put in place for the enterprise network, and it largely employs logo methods to analyses the incoming traffic of various protocols.

It generates the required breach alarms, which are also referred to as notices, and sends the signals with another device, such as SIEM.

The fundamental goal of improving security is to collect and manage IPS warnings (SIEM). The SIEM is perhaps the most widely used and dependable alternative for reviewing the acquired security assaults and reports among so many security methods. Security experts also analyze dubious signals according to rules and criteria and hunt for cruel actions by examining links across events and using threat data.

A training strategy that focuses on determining if an attack occurred in a significant amount of data may be useful for analysts who must quickly evaluate a wide variety of shows. Generally, there are two types of network antivirus: those powered by experts and that those led by computer science.

Industry best practices are based on standards developed by analysis or security experts. In the process, machine learning-based algorithms that search for odd or unexpected patterns should aid in the earlier detection of new cybercrime. Despite the reality that studying remedies are useful in discovering network in gadgets, we discovered that current student methodologies have four key limitations.

II. RELATED WORK

The massive level of Internet applications over the past 10 years has increased the need for data communications certification. As the primary line of defense for a backhaul, a management system is expected to react to the continually shifting setting. To accurately identify irregularities, researchers in the domains of image retrieval have created a range of monitored feature sets. With the aid of objects that resemble neurons, chaperoned knowledge accomplishes objectives. Back propagation has profoundly changed how people approach learning issues by generating significant advancements in a number of domains, including speech signals, object identification, and text categorization, to name a few.

This cutting-edge invention only needs to be considered for military applications.[1,2,3,4]. It aims to investigate if deep learning approaches are suitable for an anomaly-based misuse detection.

We employed a variety of deep strategy in teaching topology to develop the security testing principles for this work, including max pooling, filters, and RNN. After being taught here and on the Undulation data set, those deep determinants were taught utilizing all of the other Static qualities data points.[4,5].

Each investigation for this work was carried out by the reviewers using a software package with a GPU. Machine vision training dead center models were created using effective instructional device, nearest neighbor, j48, random forest, lda, naive ports, and linear integrand assessment. Using recognizable cut - out markers, such as sensor set points[6,7].

The testing findings of Deep IDS techniques showed promising results for their applicability in anomaly detection devices.

Insider Threat Detection, depending on an Information Schema and Assisted Directed Graph, is essential for connection awareness and invasion detection. But there are several ways to determine network intrusion, they may effectively and effectively employ super information made up of survey information with clinical knowledge[8,9,10].

Consequently, it suggests a unique detection approach based on a beliefs rule basis and a Bayesian network graph (DAG) (BRB). The Adt is used in the suggested model, known as DAG-BRB, to build a cross it's like model that may prevent an expansion of rule permutations due to a wide variety of incursion kinds[11,12]. An enhanced constraints error covariance adaptation evolution method that can successfully resolve the limitation problem as in BRB is developed to help to get the makes it possible of the DAGBRB theory[13,14].

The findings shown that the DAG-BRB model has a greater identification accuracy than other different classifiers and may be applied in actual networks. The development of an uncommon case network management is one of the primary study sub - fields of data encryption (IDS)[15].

A significant frequency (FAR) is another issue with exceptional situation IDSs, which severely limits their practical use. Utilizing deep CNNs to first know and understand limited spatial characteristics of data traffic but instead long short attention span networks to learn greater spatial highlights, we suggest a framework IDS in this study entitled the structural components functions idss system (HAST-IDS)[16].

Neural nets effectively finish the full feature language learning; featured engineering methods are not necessary. The properly learned traffic conditions considerably reduce the FAR.

And to use the industry-recognized DARPA1998 though ISCX2012 large databases, the efficacy of the proposed method is evaluated. The theory stated that HAST outperforms other existing strategies in terms of accuracy, sharpness, and FAR with both noise removal and FAR reducing[17].

III.PROPOSED METHOD

A. Proposed System

We go through earlier research on actual security interpretation and deep attempting to learn intrusion prevention. Many Artificial intelligence and machine training methods have been suggested to increase the capability of cyber threat identification in recent years, and many research in cyberspace have focused on AI-based vulnerability scanning. Although these research have used Artificial intelligence and machine continuing to learn approaches to achieve considerable results, they are still restricted to particular test datasets like NSLKDD. However, we have made use of real-world security incidents and logs. In order to solve the aforementioned difficulties, these techniques are more comparable to our own. Particularly, have utilised our technique's TF-IDF mechanism.

B. Data source

In this Raw data is collected from different types of data sourced

C. Data collection

In this stage the data is collected from different types of sources and sends to the data processing

D. Data Processing and Analysis

In this step the data is processed in to streams and Policy based Detection will be there to detect the correct data it will be send Alert if the Wrong data was passed and also in this we have AI Based detection through AI-SEM which is used to detect the Data and keep alerts and all the storage will be stored in the AI- Based detection and finally send to the Web service.

E. Data Storing and data Visualization

The data is stored in the Data base and sends to the data Visualization.

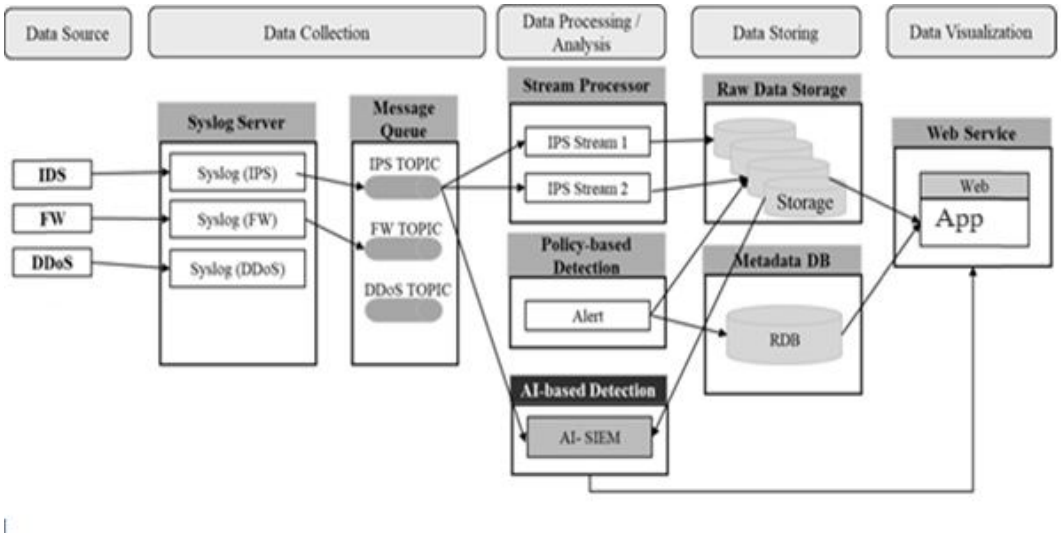


Fig 1 Architectural design

IV. DISCUSSIONS

A. Model Architecture

A quality system is someone that clearly states the scope and confirms with the closer to end user. The results of any game determine how processes results are communicated to users as well as other technologies. How information will be sent for immediate consumption or the outcome on writing is chosen upon data gathering. It is the most important and instructive instrument for that person. Economical data collecting enables communication between the processes and the costs of providing user assessment.

- Make a document, report, or other format that includes the state's information.
- An intelligence system's outputs form could achieve one or all of the goals listed below.
- Convey knowledge of previous actions, present conditions, or future predictions.
- Signal significant occurrences, chances, issues, or warnings.
- Start an action.

B. Results

We may infer from the following graph, where the x-axis shows the name of the method and the y-axis the accuracy of that methodology, that long short - term and CNN score well. Now click on Precision Comparison Graph' to get below graph

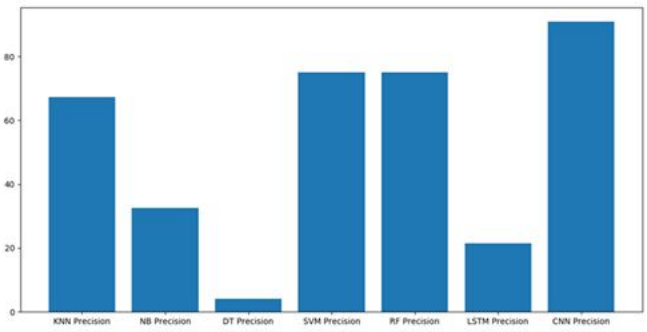


Figure 2 CNN for Precision Comparison Graph

In the below table which compares the accuracy of our genuine ESX-1 and ESX-2 sets, we can observe that the suggested EP-ANN modes perform better than the current machine-learning techniques overall. In specifics, the EP-FCNN, EP-CNN, while EP-LSTM scores for ESX-1 were 0.933, 0.952, and 0.923, respectively,

		Accuracy			
		NSLKDD	CICIDS2017	ESX-1	ESX-2
Conventional Machine Learning	SVM	0.897	0.968	0.901	0.867
	k-NN	0.909	0.978	0.905	0.858
	Random Forest	0.930	0.979	0.900	0.858
	Naive Bayes	0.698	0.621	0.692	0.616
	Decision Tree	0.919	0.979	0.900	0.858
Our Proposed Method	EP-FCNN	0.958	0.995	0.933	0.947
	EP-CNN	0.952	0.988	0.952	0.936
	EP-LSTM	0.950	0.986	0.923	0.926

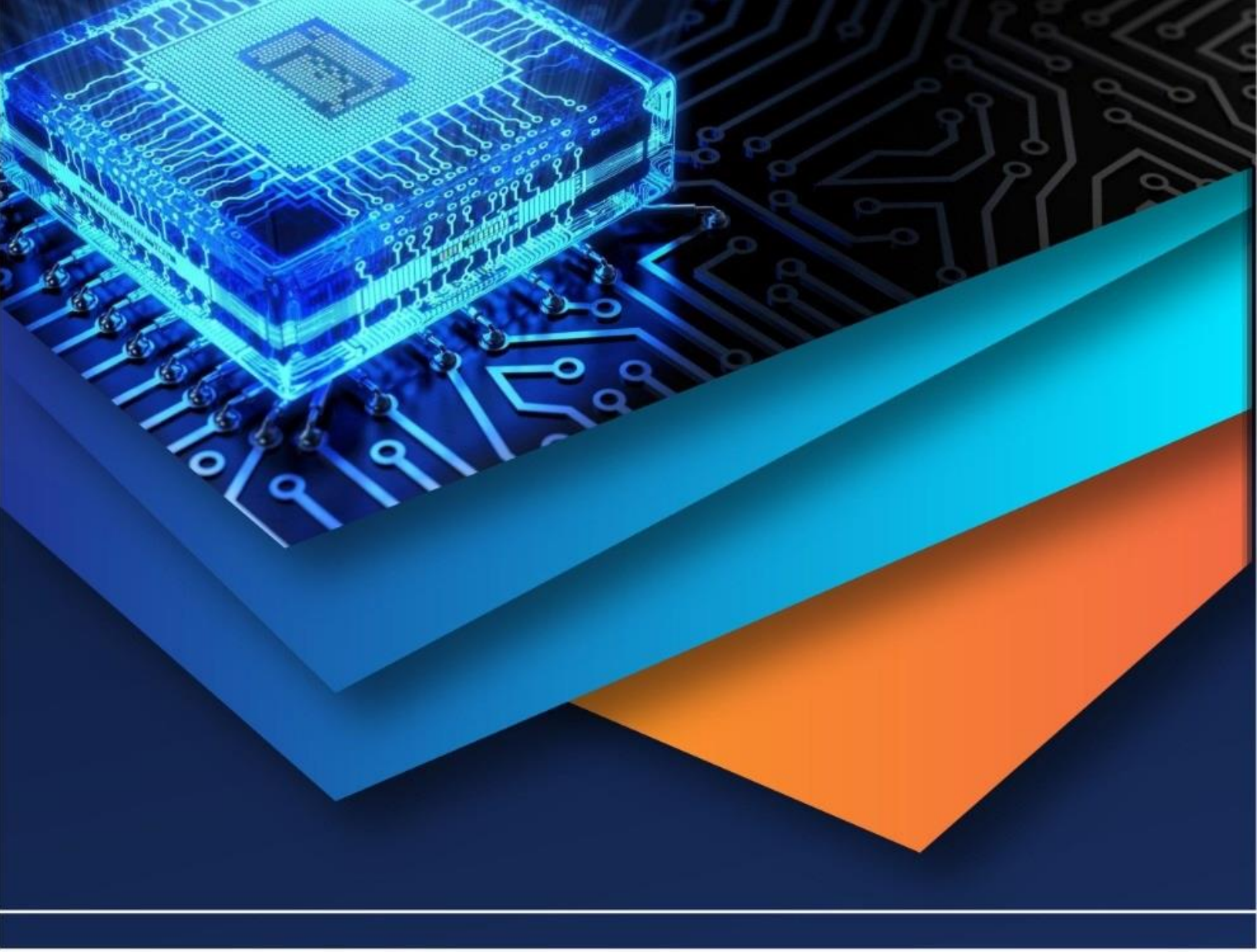
Figure 3 Test results of accuracy for various conventional machine-learning methods and our proposed

V. CONCLUSION

With the help of artificial intelligence and event profiles, we have suggested the Artificial intelligence system is easy for our approach in innovative in that it uses need plenty detection techniques to improve cyber-threat identification while condensing exceedingly huge data into events profiles. By examining long-term data assets, the AI-SIEM system allows the security professionals to respond to critical security alarms quickly and effectively.

REFERENCES

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, K. Han, "Enhanced Network Anomaly Detection Based on Deep Neural Networks," IEEE Access, vol. 6, pp. 48231-48246, 2018.
[2] 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
[3] W. Wang, Y. Sheng and J. Wang, "HAST-IDS: Learning hierarchical spatial- temporal features using deep neural networks to improve intrusion detection," IEEEAccess, vol. 6, no. 99, 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," 2015 IEEE Student Conference on Research and Development (Scored), Kuala Lumpur, 2015, pp. 305-310.
[5] 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.
[6] Hubbell and V.Surya narayana False alarm minimization techniques in signature-based intrusion detection systems: A survey,'' Compute. Common., vol. 49, pp. 1- 17, Aug. 2014.
[7] A. Naser, M. A. Majid, M. F. Zolile and S. Anwar, "Trusting cloud computing for personal files," 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, 2014, pp. 488-489.
[8] Y. Shen, E. Marconi, P. Verviers, and Gianluca Stringham, "Tiresias: Predicting Security Events Through Deep Learning," In Proc. ACM CCS 18, Toronto, Canada,2018, pp. 592-605.
[9] Kyle Soaks and Nicolas Christin, "Automatically detecting vulnerable websites before they turn malicious,", In Proc.USENIX Security Symposium., San Diego, CA,USA, 2014, pp.625-640.
[10] K. Veerama channid, I. Arnaldo, V. Koraput, C. Basis, K. Li, "AI2: training a bigdata machine to defend," In Proc. IEEE Bigdata Security HPSC IDS, New York, NY,USA, 2016, pp. 49-54
[11] 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.
[12] 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.
[13] [online] Available: http://www.takakura.com/Kyoto_data/
[14] N. Shone, T. N. Ngoc, V. D. Phail and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerge. Topics Compute. Intel., vol. 2, pp. 41-50, Feb. 2018.
[15] R. Vijayakumar, Mamoon Alazar, K. P. Soman, P. Poorna Chandran, Ameer Al- Namrata and Sit Lakshmi Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525-41550, Apr. 2019.
[16] W. Hu, W. Hu, S. Maybank, "Adaboost-based algorithm for network intrusion detection," IEEE Trans. Syst. Man B Cybern., vol. 38, no. 2, pp. 577-583, Feb. 2008.
[17] T.-F. Yen et al., "Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks", Proc. 29th Annu. Comput. Security Appl. Conf., New York, NY, USA, 2013, pp. 199- 208.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY