ISSN 2277-2685

IJESR/April-June. 2025/ Vol-15/Issue-2s/241-247

Event Profiles based Cyber Threat Detection using ANN

Bhrugubanda Venkata Lakshmi Geetha Sri
PG scholar, Department of MCA, DNR college, Bhimavaram, Andhra Pradesh.
K.RAMBABU
(Assistant Professor), Master of Computer Applications, DNR collage, Bhimavaram, Andhra Pradesh.

Abstract: ***One of the huge issues in local area security is the course of action of an automated and a hit virtual threats recognizable proof method. In this paper, we present an AI technique for virtual dangers disclosure, in gentle of fake neural associations. The suggested system changes tremendous volumes of collected threat incidents to profiles of solitary occasions and uses a major learning-essentially focused area approach for the redesign of advanced risk character. We have established an AI-SIEM framework for these works of art that is subject to a combination of Occasion profiling, such as FCNN, CNN, and LSTM, for preprocessing calculations and assorted bogus neural workplace techniques. Among prominent good and sham great cautions, the machine offices round isolate, while reassuring assurance specialists to quickly respond to virtual hazards. All tests in this exploration are done through makers utilizing two benchmark datasets (NSLKDD and CICIDS2017) and datasets amassed indeed. To confirm the introduction connection with current methodologies, we drove evaluations utilizing the 5 typical AI strategies (SVM, alright NN, RF, NB, and DT). Thusly, the test eventual outcomes of this examination guarantee that our proposed methods are prepared for being used as becoming acquainted with based styles for network interference area, and show that paying little mind to the truth that it is used in all actuality, the introduction beats the conventional AI methodologies. In this paper author is describing concept to detect threats using AI-SIEM (Artificial Intelligence-Security Information and Event Management) technique which is a combination of deep learning algorithms such as FCNN, CNN (Convolution Neural Networks) and LSTM (long short term memory) and this technique works based on events profiling such as attack signatures. Author evaluating propose work performance with conventional algorithms such as SVM, Decision Tree, Random Forest, KNN and Naïve Bayes. Here I am implementing CNN and LSTM algorithms.***

Index terms : Cyber wellbeing, interference zone, local area security, man-made cognizance, significant neural offices.

I. INTRODUCTION

competence (AI) techniques, reading basically based approaches for recognizing virtual attacks are getting also progressed, and they have performed fundamental outcomes in various examinations. In any case, by virtue of persistently progressing computerized attacks, it's far by the by beautiful looking at to comfortable IT structures against chances and vindictive practices in organizations. By virtue of different organization interferences and pernicious games, convincing protections and security thoughts were given extreme requirement for discovering strong arrangements. For the most part, there are two basic systems for perceiving virtual dangers and business venture interferences.

An interference expectation system (IPS) is conveyed inside the endeavor business, and may inspect the partnership shows and streams with signature-based absolutely procedures fundamentally. It makes appropriate interference alerts, alluded to as the wellbeing exercises, and audits the creating alerts to some other structure, as a case, SIEM. The wellbeing records and even the board amassing extreme broadly recognized plan exceptional wellbeing exercises answers for investigate the accumulated security exercises and logs [5]. Also, security agents put forward an attempt to investigate far-fetched alerts through systems and feature, and to find poisonous lead via separating associations among occasions, using realities perceived with assaults.

Regardless, it is as yet extreme to see and recognize interferences towards shrewd boss attacks inferable from their unreasonable counterfeit enormous level. Therefore, cutting edge examinations region interference ID concentrated on AI and programmed thinking procedures for sorting out assaults. Movement in AI fields can support the assessment of organization interferences with the guide of insurance experts in a helpful and robotized way. These acquiring information on based philosophies need to take inside the assault model from chronicled hazard data and use the readied styles to perceive

interferences for hard to comprehend virtual dangers [8], [9]. An examining essentially based methodology assumed for sorting out if an attack happened to in a ton of data might be valuable to experts who need to in a brief moment review different exercises. As in sync with [10], insights security plans for the most extreme component fall into two orders: inspector pushed and AI driven courses of action. Inspector pushed arrangements rely on recommendations made do with the guide of wellbeing specialists known as trained professionals.

In the mediating time, AI driven courses of action used to see remarkable or odd models can improve character of most recent computerized risks [10]. By and through, simultaneously as dominating based strategies are valuable in recognizing virtual assaults in structures and organizations, we saw that contemporary becoming more acquainted with based absolutely approaches have four essential cutoff points. In any case, dominating based absolutely area systems require checked information, which enable the act of the adaptation and assessment of made acquiring information on models. In addition, it isn't clear to get such stamped records at a scale that license novel preparing of a form. Despite the prerequisite for stamped realities, severa endeavor SIEM courses of action don't protect up named data that can be actualized to coordinated dominating styles [10].

Second, the extra a piece dominating applied every test summarized truth be told, given that they might be like way. Consequently, hard apply moderate. Continuous undertakings interference region a robotization technique significant becoming acquainted with headways, and execution has been surveyed using amazing. Nevertheless, various past examinations applied benchmark dataset, which, however genuine, aren't generalizable to this blessing actuality due to the lacking features. To win over those limitations, a used acquiring information on model wishes to survey with datasets which may be gathered in truth. Third, using an eccentricity based way to deal with recognize network interference can help comprehend hard to comprehend virtual dangers; while it can similarly reason a high counterfeit alert rate [6].

II. LITEARTURE SURVEY

[1] Saleem, Y., & Bashir, M. K. (2018)
In their study on enhanced network anomaly detection, Saleem and Bashir explored the application of deep neural networks (DNNs) to intrusion detection systems (IDS), aiming to improve detection accuracy in the face of evolving cyber threats. Utilizing models like Convolutional Neural Networks (CNN), Autoencoders, and Recurrent Neural Networks (RNN), they trained and tested their architectures on the NSLKDD dataset and demonstrated improved performance in anomaly detection compared to traditional machine learning methods. The study highlighted the advantage of using DNNs for automatic feature extraction and better generalization, which led to high accuracy and robust performance in real-time network intrusion environments. This work emphasizes the promising role of deep learning for enhancing the capabilities of IDS in detecting both known and unknown attacks.

[2] Network Intrusion Detection Based on Directed Acyclic Graph and Belief Rule Base (2017)
This paper introduced a novel approach for intrusion detection using a Directed Acyclic Graph (DAG) integrated with a Belief Rule Base (BRB), called DAG-BRB. The DAG structure enabled a hierarchical and multi-layered representation of rules to address the scalability issues posed by a large set of intrusion scenarios. The use of a Covariance Matrix Adaptation Evolution Strategy (CMA-ES) further optimized the system's parameters, improving its accuracy and adaptability. Experimental evaluations showed that DAG-BRB outperformed traditional models in terms of detection rates, particularly due to its ability to handle uncertainty and complex rule combinations effectively. This methodology presents a strong framework for intelligent and adaptive IDS design.

[3] HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks
The HAST-IDS model was developed to overcome

limitations in traditional IDS by learning both spatial and temporal features from raw network traffic using deep learning architectures. This approach utilized Convolutional Neural Networks (CNNs) to capture spatial patterns and Long Short-Term Memory (LSTM) networks for temporal behavior learning, thereby enabling more accurate anomaly detection without manual feature engineering. Evaluated on DARPA1998 and ISCX2012 datasets, HAST-IDS demonstrated superior performance with reduced false alarm rates and higher detection accuracy. The method sets a new standard by leveraging hierarchical feature extraction directly from raw input, making it effective for identifying complex, time-dependent intrusions.

[4] Hussein, M. K., & Jaber, A. N. (2015)
Hussein and Jaber proposed a security analysis framework for cloud-based networks using honeypot technology to combat DDoS attacks. Their system focused on using research-oriented honeypots for behavior analysis of potential attackers in virtualized environments. The study stressed the importance of proactive security mechanisms, particularly in cloud computing, where sensitive data is frequently at risk. The proposed model offers a method to monitor, trap, and analyze attack vectors, aiding in the formulation of more robust defense strategies. This research underscores the growing need for intelligent intrusion tracking tools as cloud services become increasingly prevalent.

[5] Profiling SIEM Tools and Correlation Engines for Security Analytics
This work analyzed and compared Security Information and Event Management (SIEM) tools, focusing on their ability to collect, correlate, and analyze security event data. The paper provided a comparative profile of widely used SIEM platforms and correlation engines, emphasizing their role in real-time threat detection and incident response. The authors discussed how effective SIEM systems enhance organizational security by providing centralized visibility and automated analytics. This review supports the selection and deployment of SIEM tools that align with specific enterprise security requirements and demonstrates their increasing importance in modern cybersecurity infrastructures.

[6] Suryanarayanan, V., & Hubballiand, N. (2014)
In their comprehensive survey, Suryanarayanan and Hubballiand examined various techniques for minimizing false alarms in signature-based intrusion detection systems. The authors classified and evaluated methods such as alert correlation, pattern clustering, and neural network-based filtering. They highlighted the persistent challenge of balancing detection sensitivity and false positive reduction. The survey provided valuable insights into both academic approaches and their practical implementation in SIEM tools. This work is particularly relevant to IDS developers aiming to enhance detection reliability while maintaining system efficiency

[7] Trusting Cloud Computing for Personal Files (2014)
This study addressed key security concerns in cloud computing, particularly related to the storage and management of personal and sensitive information. It discussed vulnerabilities in current cloud storage systems and proposed strategies to improve data confidentiality and integrity. The paper emphasized the societal implications of cloud security, including the potential for large-scale disruptions in urban digital infrastructure. The authors highlighted real-world applications such as IBM's Smarter Cities and Cisco's Busan initiative, demonstrating the potential of secure cloud solutions to support urban mobility, energy management, and public services. This research forms a crucial foundation for trust-building in widespread cloud adoption.

III. PROPOSED METHOD

In this paper author is describing concept to detect threats using AI-SIEM (Artificial Intelligence-Security Information and Event Management) technique which is a combination of deep learning algorithms such as FCNN, CNN (Convolution Neural Networks) and LSTM (long short term memory) and this technique works based on events profiling such as attack signatures.

Author evaluating propose work performance with conventional algorithms such as SVM, Decision Tree, Random Forest, KNN and Naïve Bayes. Here I am implementing CNN and LSTM algorithms.

Propose algorithms consists of following module

1) Data Parsing: This module take input dataset and parse that dataset to create a raw data event model

2) TF-IDF: using this module we will convert raw data into event vector which will contains normal and attack signatures

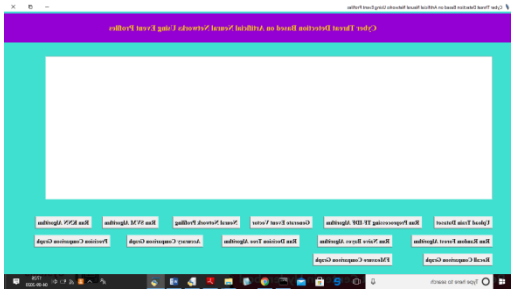
3) Event Profiling Stage: Processed data will be splitted into train and test model based on profiling events.

4) Deep Learning Neural Network Model: This module runs CNN and LSTM algorithms on train and test data and then generate a training model. Generated trained model will be applied on test data to calculate prediction score, Recall, Precision and F Measure. Algorithm will learn perfectly will yield better accuracy result and that model will be selected to deploy on real system for attack detection.

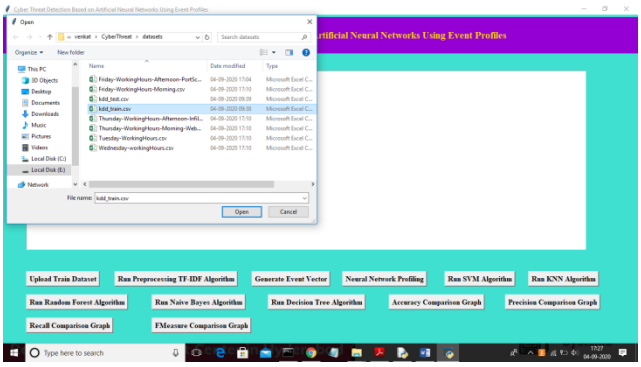
Datasets which we are using for testing are of huge size and while building model it's going to out of memory error but kdd_train.csv dataset working perfectly but to run all algorithms it will take 5 to 10 minutes. You can test remaining datasets also by reducing its size or running it on high configuration system.

IV. RESULTS

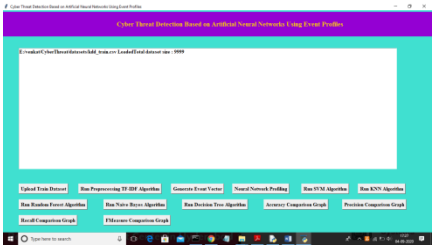
To run project double click on 'run.bat' file to get below screen



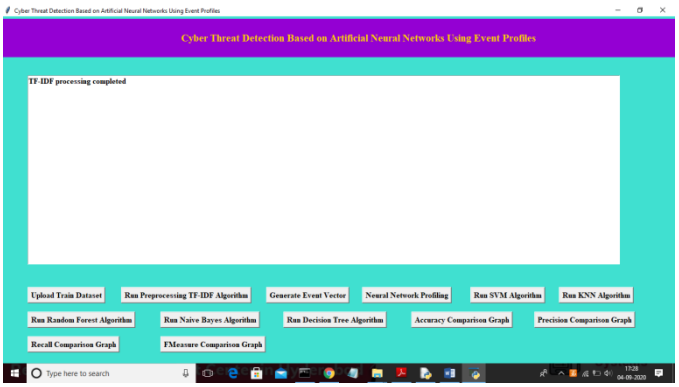
In above screen click on 'Upload Train Dataset' button and upload dataset



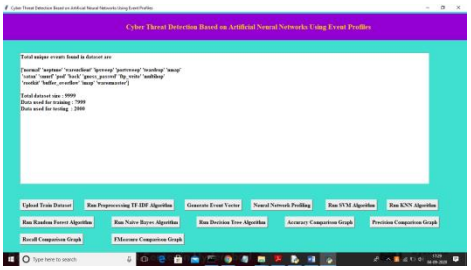
In above screen uploading 'kdd_train.csv' dataset and after upload will get below screen



In above screen we can see dataset contains 9999 records and now click on 'Run Preprocessing TF-IDF Algorithm' button to convert raw dataset into TF-IDF values



In above screen TF-IDF processing completed and now click on 'Generate Event Vector' button to create vector from TF-IDF with different events

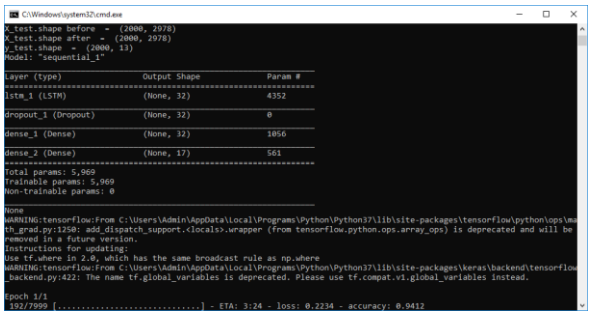


In above screen we can see total different unique events names and in below we can see dataset total size and application using 80% dataset (7999

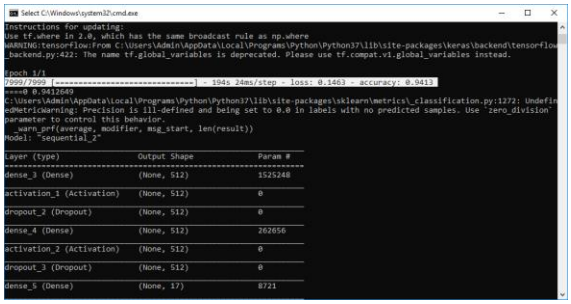
ISSN 2277-2685

IJESR/April-June. 2025/ Vol-15/Issue-2s/241-247

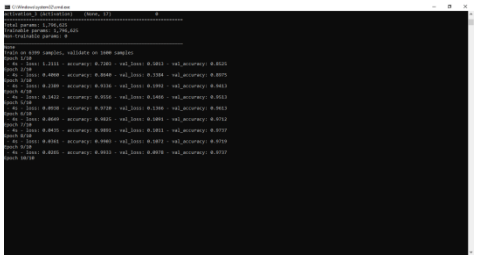
records) for training and using 20% dataset (2000 records) for testing. Now dataset train and test events model ready and now click on 'Neural Network Profiling' button to create LSTM and CNN model



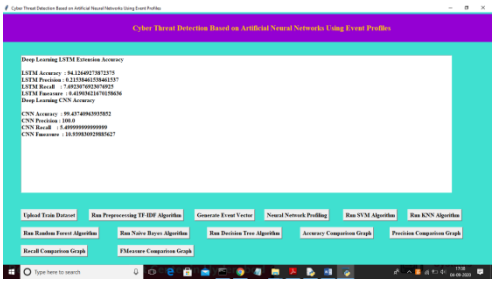
In above screen LSTM model is generated and its epoch running also started and its starting accuracy is 0.94. Running for entire dataset may take time so wait till LSTM and CNN training process completed. Here dataset contains 7999 records and LSTM will iterate all records to filter and build model.



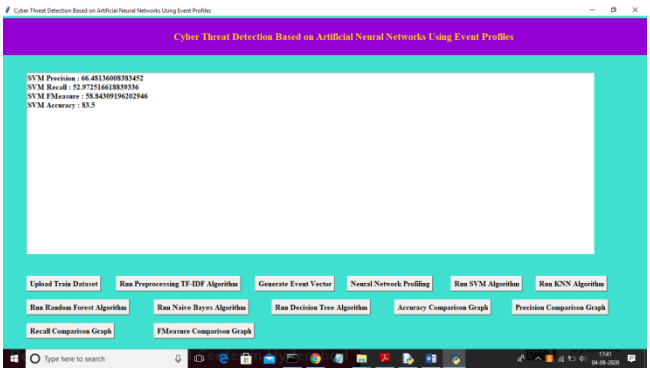
In above selected text we can see LSTM complete all iterations and in below lines we can see CNN model also starts execution



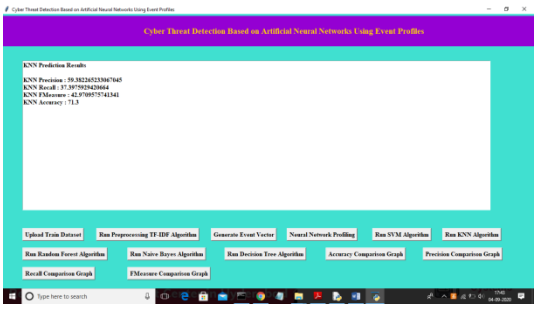
In above screen CNN also starts first iteration with accuracy as 0.72 and after completing all iterations 10 we got filtered improved accuracy as 0.99 and multiply by 100 will give us 99% accuracy. So CNN is giving better accuracy compare to LSTM and now see below GUI screen with all details



In above screen we can see both algorithms accuracy, precision, recall and FMeasure values. Now click on 'Run SVM Algorithm' button to run existing SVM algorithm



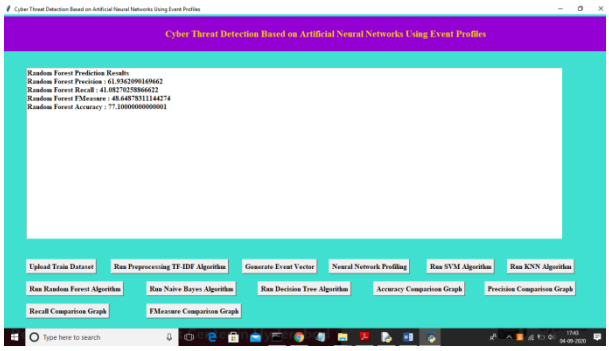
In above screen we can see SVM algorithm output values and now click on 'Run KNN Algorithm' to run KNN algorithm



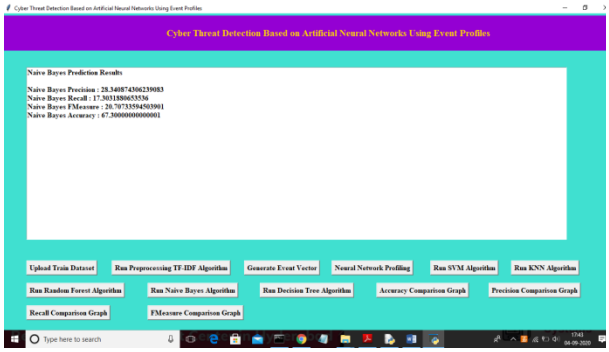
In above screen we can see KNN algorithm output values and now click on 'Run Random Forest Algorithm' to run Random Forest algorithm

ISSN 2277-2685

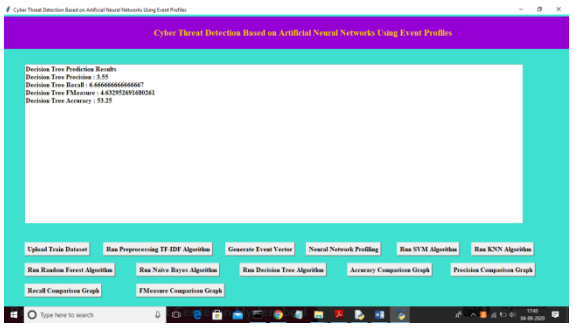
IJESR/April-June. 2025/ Vol-15/Issue-2s/241-247



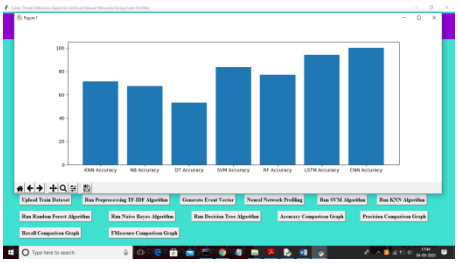
In above screen we can see Random Forest algorithm output values and now click on 'Run Naïve Bayes Algorithm' to run Naïve Bayes algorithm



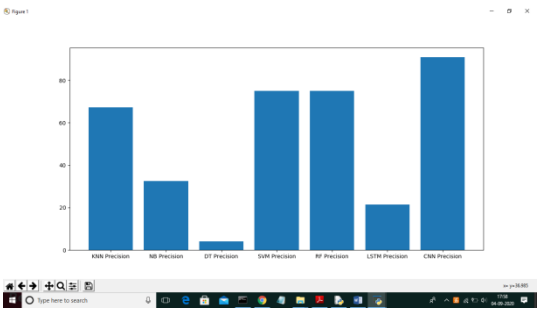
In above screen we can see Naïve Bayes algorithm output values and now click on 'Run Decision Tree Algorithm' to run Decision Tree Algorithm



Now click on 'Accuracy Comparison Graph' button to get accuracy of all algorithms

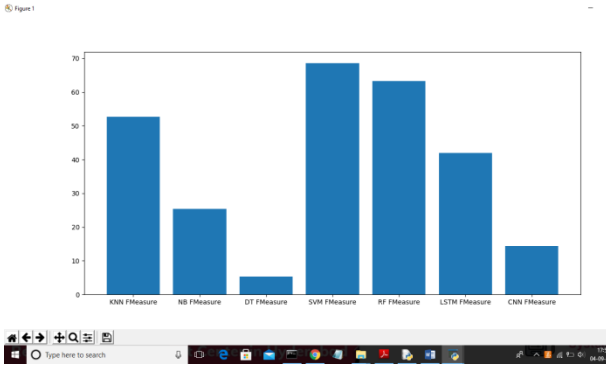


In above graph x-axis represents algorithm name and y-axis represents accuracy of those algorithms and from above graph we can conclude that LSTM and CNN perform well. Now click on Precision Comparison Graph' to get below graph



In above graph CNN is performing well and now click on 'Recall Comparison Graph'

In above graph LSTM is performing well and now click on FMeasure Comparison Graph button to get below graph



From all comparison graph we can see LSTM and CNN performing well with accuracy, recall and precision.

V. CONCLUSION

In this paper, we've proposed the AI-SIEM structure utilizing event profiles and artificial neural organizations. The peculiarity of our work lies in gathering very monstrous degree records into event profiles and using the significant contemplating based absolutely personality methods for redesigned virtual danger disclosure capacity. The AI-SIEM system enables the security examiners to oversee tremendous wellbeing alerts quickly and accurately with the guide of differentiating protracted take security records. By reducing false brilliant cautions, it might similarly help the security analysts to quick respond to computerized hazards dissipated all through endless wellbeing occasions.

REFERENCES

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, K. Han, "Overhauled 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. Qiao, L. Chang, "Association 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 progressive spatial-transient features utilizing significant neural offices to improve interference revelation," IEEE Access, vol. 6, no. 99, pp. 1792-1806, 2018.

[4] M. K. Hussein, N. Compartment Zainal and A. N. Jaber, "Data security research for DDoS assurance of cloud based absolutely organizations," 2015 IEEE Student Conference on Research and Development (SCOReD), Kuala Lumpur, 2015, pp. 305-310.

[5] S. Sandeep Sekharan, K. Kandasamy, "Profiling SIEM instruments and association engines for security test," In Proc. Int. Conf. Far off Com., Signal Proce. Besides, Net.(WiSPNET), 2017, pp. 717-721.

[6] N.Hubballiand V.Suryanarayanan,"False ready minimization strategies in imprint based absolutely interference notoriety structures: A glance at," Comput. Commun., vol. 49, pp. 1-17, Aug. 2014.

[7] A. Naser, M. A. Majid, M. F. Zolkipli and S. Anwar, "Accepting administered registering for individual archives," 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, 2014, pp. 488-489.

[8] Y. Shen, E. Mariconti, P. Vervier, and Gianluca Stringhini, "Tiresias: Predicting Security Events Through Deep Learning," In Proc. ACM CCS 18, Toronto, Canada, 2018, pp. 592-605. [9] Kyle Soska and Nicolas Christin, "Normally sorting out powerless locales before they turn noxious,", In Proc. USENIX Security Symposium., San Diego, CA, USA, 2014, pp.625-640. [10] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, K. Li, "AI2: preparing an essential data gadget to monitor," In Proc. IEEE BigDataSecurity HPSC IDS, New York, NY, USA, 2016, pp. 49 54