ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2s/467-473
Janni Narendra *et. al.*, / International Journal of Engineering & Science Research

CYBER THREAT DETECTION BASED ON ARTIFICIAL NEURAL NETWORKS USING EVENT PROFILES

Janni Narendra
PG scholar, Department of MCA, DNR College, Bhimavaram, Andhra Pradesh.
Ch.Jeevan Babu
(Assistant Professor), Master of Computer Applications, DNR college, Bhimavaram, Andhra Pradesh.

Abstract:

In this study, we present an artificial intelligence (AI) strategy for identifying cyber hazards that is based on artificial neural networks. We developed an AI-SIEM solution for this project that integrates event profiling for data pre-treatment with a variety of artificial neural network approaches, including LSTM, CNN. The method makes it very easy for security experts to distinguish real false positive signals from positive signals, allowing them to respond to cyber-attacks quickly. The CICIDS2017 and NSLKDD benchmark datasets are used as well as two real-world datasets for each experiment in this research. To compare the performance of the five traditional machine-learning algorithms (DT, NB, RF, k-NN, and SVM), we conducted tests using them. The experimental findings in this research support the usage of the suggested techniques as learning-based network models for intrusion demonstration and detection, showing that they outperform traditional machine learning techniques when used in practical settings.

INDEX TERMS: deep neural networks, artificial intelligence, intrusion detection, network security, Cyber security.

I. INTRODUCTION

Due to frequent network intrusions and harmful actions, effective security and defence concerns were given top priority for creating reliable solutions [1]–[4].

On the enterprise network, an IPS is installed, and it typically employs signature-based methods to keep track of network flows and protocols. The SIEM is the most well-liked and dependable option for studying the gathered security events and logs among the various security operations solutions [5]. Security analysts also look into suspicious warnings based on policies and thresholds, and they apply attack-related data to investigate correlations between occurrences and look for malicious behaviour.

Security professionals can quickly and automatically evaluate network assaults with the use of AI-related domain development. The attack model must be learned from previous threat data for these learning-based approaches, and trained models must be used to find incursions for unidentified cyber threats [8], [9].

Analysts that need to swiftly assess a big number of occurrences may benefit from a learning-based technique that focuses on detecting whether an assault occurred in a huge amount of data. [10]

Analyst-driven approaches are based on standards developed by analysts, or security experts. Meanwhile, systems powered by machine learning that look for uncommon or unusual patterns can help identify future cyber threats better [10]. We discovered that while existing learning-based strategies are helpful for detecting cyberattacks in systems and networks, they have four major drawbacks.

First, labelled data are necessary for learning-based detection techniques since they allow for model training and evaluation. Furthermore, obtaining such labelled data at a scale that enables precise model training is difficult.

Third, a significant percentage of false alarms may result from utilising an anomaly-based technique to identify network intrusion, which may assist expose undiscovered cyber risks. [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.

II. LITERATURE SURVEY

There are a few methods for detecting network intrusion, but they cannot directly and effectively employ semi-quantitative data, which

combines quantitative data and expert knowledge. Therefore, this study proposes a novel belief rule-based and directed acyclic graph (DAG) based detection model. The proposed model, DAG-BRB, builds a multi-layered BRB model using the DAG to avoid an explosion of rule number combinations caused by a range of intrusion types. The effectiveness of the suggested DAG-BRB was evaluated using a case study. The findings demonstrated that the DAG-BRB model has a greater detection rate than other detection models and may be applied in actual networks. [2]

IDS may identify innovative and previously unknown threats by analysing network data to distinguish between normal and abnormal behaviour. However, how well an IDS performs is significantly influenced by the way its features are designed, and there is currently no consensus on how to create a feature set that can precisely describe network traffic. A high FAR is another issue with anomaly-based IDSs, which severely limits their practical use. Deep neural networks automatically finish the full feature learning process; feature engineering methods are not necessary. [3].

IT companies today produce enormous amounts of data. In the realm of IT, handling large data blobs is crucial in and of itself. As a result, centralising the log management system boosts security in an organisation while also improving data protection. To increase the bar on security, these companies want a prominent tool that helps manage information and event data. The security analysis method Security Information and Event Management (SIEM) emphasises a comprehensive view of security in an organisation. All files and data from the various devices are collected, examined, normalised, and correlated by SIEM systems, which also provide a centralised view of logs. The open source rule-based and most popular SIEM tools correlation engines are profiled in this article, along with an overview of SIEM products and event correlation engines and a technical comparison of both. [5]

A network-based IDS, which collects and examines network traffic, alerts the system administrator of any potential low-level security breaches. These low level and incomplete reports become unmanageable to the administrator in a large network system, which results in certain unattended incidents. Modern IDS are also widely known for producing a high number of false alarms. False alarm reduction techniques are widely used in commercial SIEM products and are regularly recommended in IDS literature. This article reviews the methods for lowering false alarms in signature-based NIDS. We suggest taxonomy of methods for signature-based IDS false alarm reduction, along with the benefits and drawbacks of each type. [6]

Artificial intelligence is a new technology today. Currently, numerous applications leverage neural network concepts. Both the amount of internet usage and the absence of security are growing daily. Phishing schemes are most prevalent when it comes to network security. The use of neural network principles in the realm of network security has been briefly described in this study along with how to train and evaluate data using artificial neural networks. supervised learning model, sigmoid transfer function, gradient descent momentum training goal, and Feed forward back propagation network structure are some of the characteristics that were used to train the model for predicting fraudulent assaults. [7]

III. PROPOSED METHOD

The concept of threat detection is discussed in this paper using the AI-SIEM technique. This technique combines deep learning algorithms like LSTM, CNN and FCNN, it is based on events profiling, like attack signatures. To assess the effectiveness of the suggested work, the author employs conventional approaches including Naive Bayes, KNN, RF, Decision Tree, and SVM. I'm using the LSTM and CNN algorithms here.
Propose algorithms consists of following module

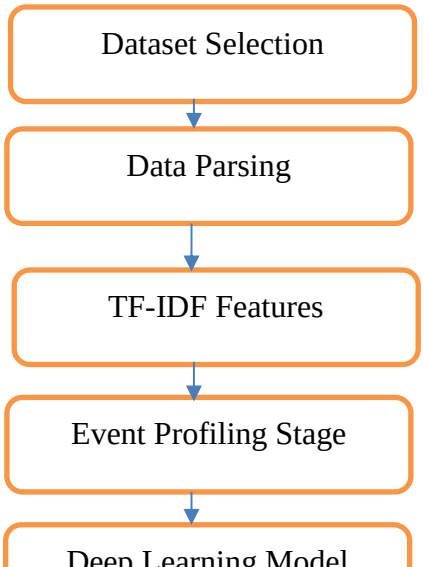

Fig.1 Flow chart of proposed system

1) Data Parsing: To generate a raw data event model, this module parses the incoming dataset.

2) TF-IDF: We will transform unprocessed data by utilising this module, into event vectors that contain both attack and normal signatures.

3) Event Profiling Stage: The data is split into test data and, based on profiling events, training data.

4) Deep Learning Neural Network Model: These modules use the LSTM and CNN algorithms to test and training data to produce a training model.

On test data, the generated trained model will be used to determine the FMeasure, precision, recall, and prediction score. When an algorithm learns properly, the results are more accurate, and that model is chosen for attack detection used in a real system. The test datasets we are using are very large, and when developing a model, there will be an out of memory error, however the kdd_train.csv dataset is working flawlessly, though it will take 5 to 10 minutes to execute all methods.

IV. RESULT

To get below screen double click on ‘run.bat’ file to run project,

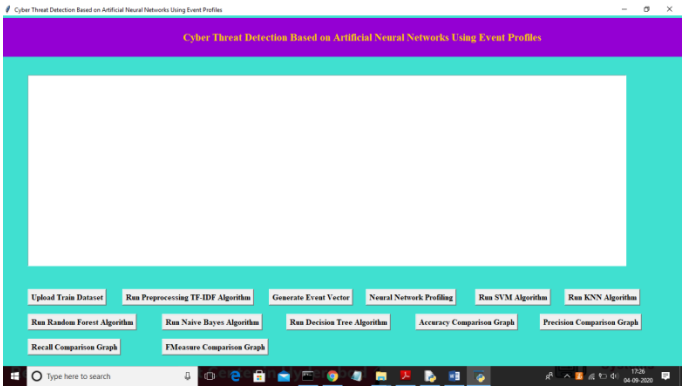

Fig.2 Run.bat file

Click the "Upload Train Dataset" button in the aforementioned screen to upload the dataset.

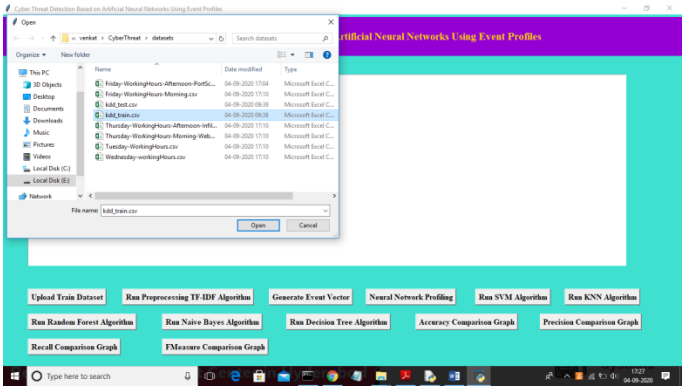

Fig.3 ‘kdd_train.csv’ dataset

'kdd_train.csv' dataset is being uploaded in the previous screen; after done, the screen below will appear.

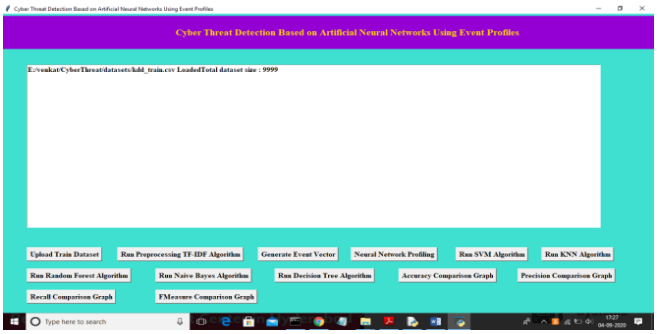

Fig.4 Dataset

As seen in the screen above, the dataset contains 9999 records. To transform the raw dataset into TF-IDF values, click the "Run Pre-processing TF-IDF Algorithm" button.

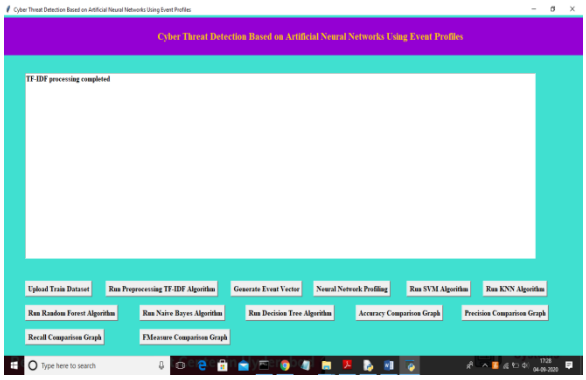

Fig.5 completion of TF-IDF processing

The processing of the TF-IDF has been completed in the screen above. Click the "Generate Event Vector" button to produce a vector from the TF-IDF with various events.

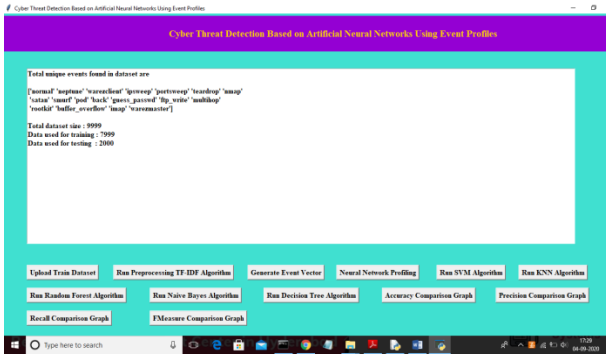

Fig.6 different unique events names

In the screen above, we can see a list of all the unique event names, and in the screen below, we can see the dataset's overall size and the application's usage, which uses 20% (2000 records) for testing and 80% of the dataset (7999 records) for training. Now that the dataset has been prepared for testing and training, establish an CNN and LSTM model by clicking the "Neural Network Profiling" button.

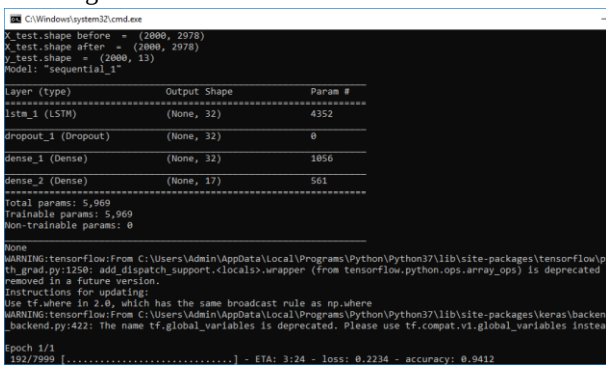

Fig.7. Generation of LSTM model

In the screen above, the LSTM model has been built, its epoch running has started, and its initial accuracy is 0.94. Wait until LSTM and CNN training is complete before running the entire dataset. This dataset has 7999 records, and the LSTM iterates over each record to filter and construct the model.

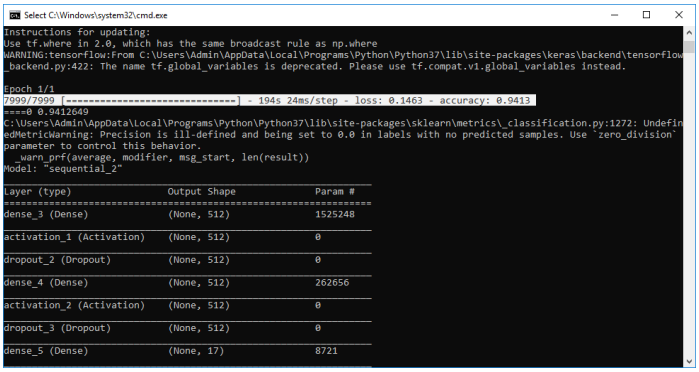

Fig.8 LSTM complete all iterations

The LSTM in the highlighted paragraph above completes all iterations, and the CNN model begins execution in the lines below.

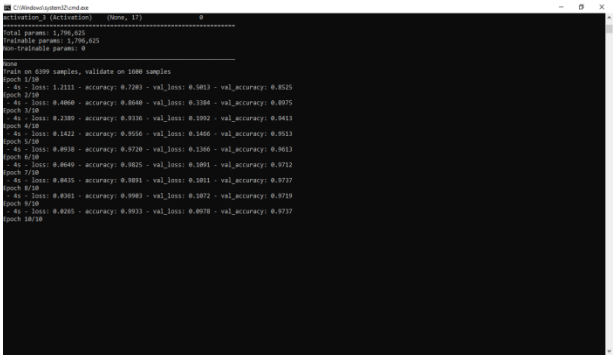

Fig.9. CNN start the iteration

In the example above, CNN also starts with an accuracy of 0.72 after the first iteration, and after 10 iterations, we obtain a filtered improved accuracy of 0.99, which we can multiply by 100 to get an accuracy of 99%. Consequently, CNN offers greater accuracy in comparison to LSTM. To see the whole GUI interface, click below.

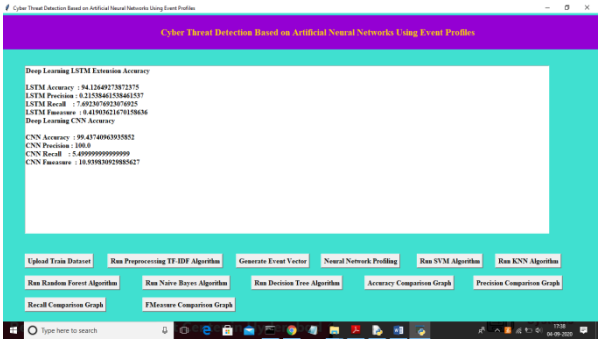

Fig.10. accuracy, precision, recall and FMeasure values

FMeasure, recall, precision, and Accuracy, values for the algorithms are displayed in the screen

above. To run the current SVM algorithm, click the "Run SVM Algorithm" button now.

Fig.11. output values of SVM algorithm

We can see the results of the SVM algorithm on the screen above. Click "Run KNN Algorithm" to start the KNN algorithm.

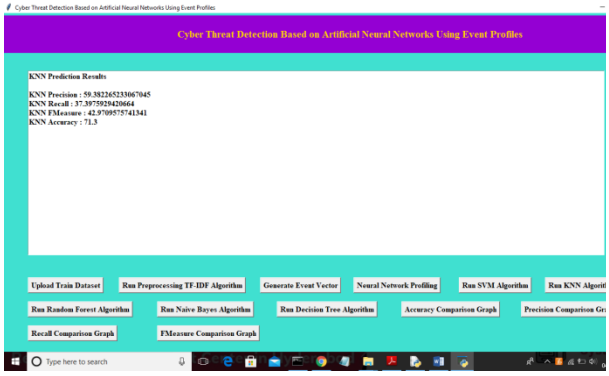

Fig.12 output values of KNN algorithm

The output of the SVM algorithm is displayed on the screen above. To launch the KNN algorithm, click "Run KNN Algorithm.

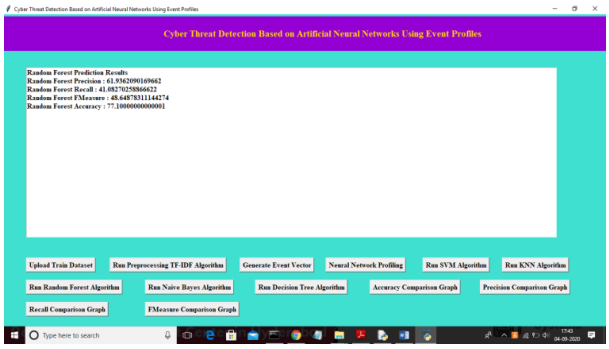

Fig.13 output values of Random Forest algorithm

We can see the results of the Random Forest method in the screen above. To run the NB algorithm, click the "Run Naive Bayes Algorithm" button.

Fig.13 output values of Naïve Bayes algorithm

Click "Run Decision Tree Algorithm" to launch the DT Algorithm after viewing the output values of the Naive Bayes algorithm in the previous screen.

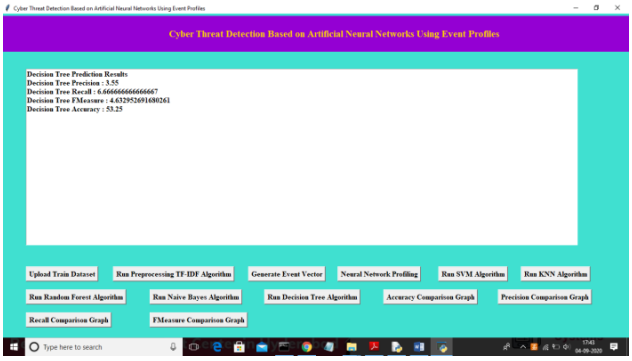

Fig.13 output values of DT algorithm

To view the accuracy of all algorithms, click the "Accuracy Comparison Graph" button now.

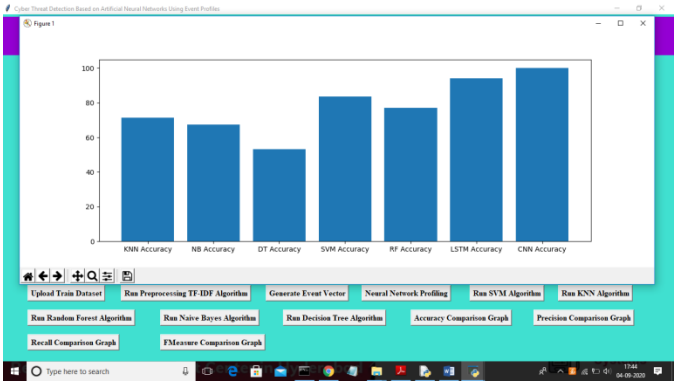

Fig.14 Accuracy Comparison Graph

The accuracy of the algorithms is shown on the y-axis in the graph above, while the algorithm names are on the x-axis. It is clear from the graph that the algorithms CNN and LSTM perform well.

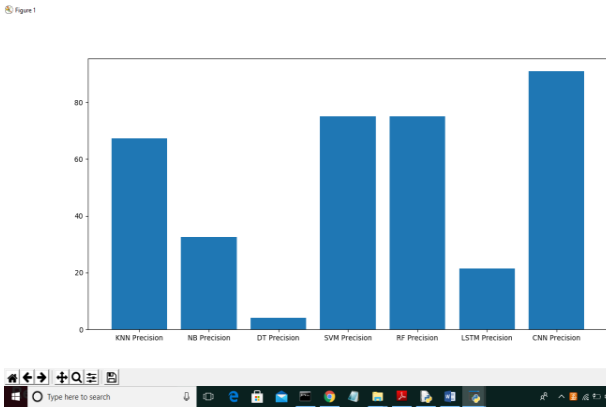

Fig.15 Precision Comparison Graph

Click on the "Recall Comparison Graph" link to see how CNN is performing in the graph above.

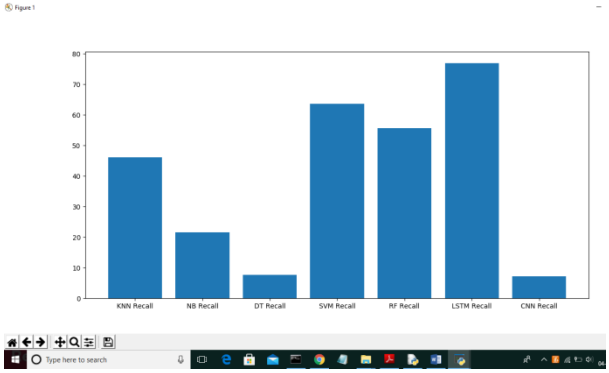

Fig.16 Recall Comparison Graph

The LSTM is functioning properly in the previous graph.

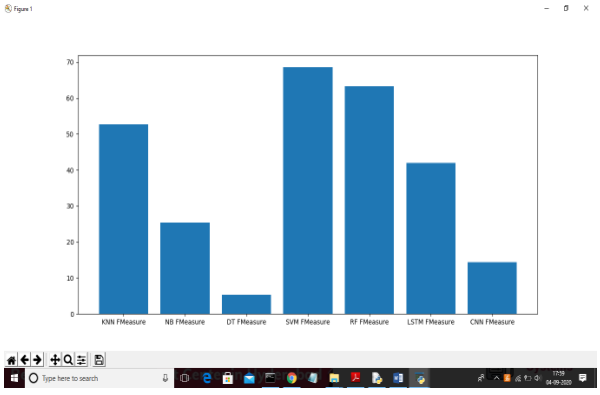

Fig.17 FMeasure Comparison Graph

The complete comparison graph shows that LSTM and CNN are performing well in terms of precision, recall and accuracy.

V. CONCLUSION

Our approach is unusual in that it boosts cyber-threat identification utilising deep learning-based detection algorithms while compressing very large-scale data into event profiles. We developed an AI-SIEM solution for this project that integrates event profiling for data pre-treatment with a variety of artificial neural network approaches, including LSTM, CNN, and FCNN. The technology puts a lot of emphasis on telling actual false positive warnings from positive signals, enabling security analysts to react to cyber threats quickly. The CICIDS2017 and NSLKDD benchmark datasets are used as well as two real-world datasets for each experiment in this research. To compare the performance of the five traditional machine-learning algorithms (DT, NB, RF, k-NN, and SVM), we conducted tests using them. The experimental findings in this research support the usage of the suggested techniques as learning-based network models for intrusion demonstration and detection, showing that they outperform traditional machine learning techniques when used in practical settings.

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.