IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Advanced Event-Based Cyber Threat Detection With Cnn And Lstm

[1]Devarakonda Ramavamsi, Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions

[2]Mrs. K Baby Kumari, Assistant Professor at Miracle Educational Society Group of Institutions

[3]Panigrahi Asish Kumar, Assistant Professor at Miracle Educational Society Group of Institutions

ABSTRACT

In this work, we propose an ANN-based AI cyber security framework for detecting cyber attacks. By converting security incidents into single entities, the architecture takes advantage of advanced learning models including CNN and LSTM to improve the detection rate of the system. The AI-SIEM system decreases the occurrence of false alarms, thus enabling more efficient and faster response to changing cyber attacks. Experiments carried out on benchmark datasets, such as NSLKDD, CISIDS2017, results high values when compared to other machine learning techniques like SVM, k-NN and Decision Trees. The technique in question has been designed with an emphasis on practical scenarios, where issues such as data annotation and overfitting are expected. The results confirm that the elaborated framework is competent enough for intrusion detection, working with large volumes of information and responding to a changing threat landscape, thus providing strong defense in various spheres of cybersecurity.

Keywords: LSTM, k-NN, SVM

INTRODUCTION:

The threats raised in the cyber space seem to have become advanced and this has posed problems to the conventional alarm systems to be able to monitor the more complex and sophisticated attacks in an efficient manner. Conventional strategies which depend on the use of static algorithms or predefined rules find it hard to cope with low rates of false positives and their resistance to changes in the patterns of attacks. Technologies related to machine learning and AI on their part look to offer better opportunities by using data driven models for automatic identification of anomalies. This project presents and develops a new model that combines deep learning models such as CNN and LSTM networks and event profiling in detecting cyber threats. This system is unlike the previous methods which aim at transforming security events into structured profiles, thus a more accurate classification of threats is achieved. The framework uses benchmark datasets like NSLKDD and CICIDS2017 and manages to achieve better attack detection rates and thus the systems have promise for real world use. This gap of tackling the issues of adaptability and scalability is critical to achieving building large scale cybersecurity systems.

GAP IDENTIFIED BASED ON LITERATURE SURVEY:

The literature review exposes massive gaps in the current cyber threat detection systems. Traditionally, Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems were based on either some signature-based approaches or on older forms of machine learning such as SVM and Decision Trees. These approaches usually have high false positives rates, poor scalability and difficulty in dealing with dynamic targets. In addition, most models use labeled datasets to train, and such datasets are in most cases absent in real life, limiting their applicability.

Another major gap is related to the automated processing of complicated and high-dimensional data representations. This is despite benchmark datasets like NSLKDD and CICIDS2017 providing initial test environments. Additionally, classic feature engineering does not define the time tags, and that ignores the intricate dependencies of the events.

Although some of the barriers have been overcame by the deep learning CNN, LSTM for some reason they are not widely used in event-based profile for the threat detection. Limited research has investigated the hybrid models which combine different deep learning frameworks with studying the issue of precision vs recall bias. The objectives of the study close these gaps, through AI-SIEM models that use an event profiling and ANN to improve threat detection efficacy and its range across a wide area of cybersecurity environments.

PROBLEM STATEMENT:

Cyber risk management is often unsatisfactory due to the presence of a high level of false positives, slow rates of reaction, and inability to provide flexibility as per redefined parameters.

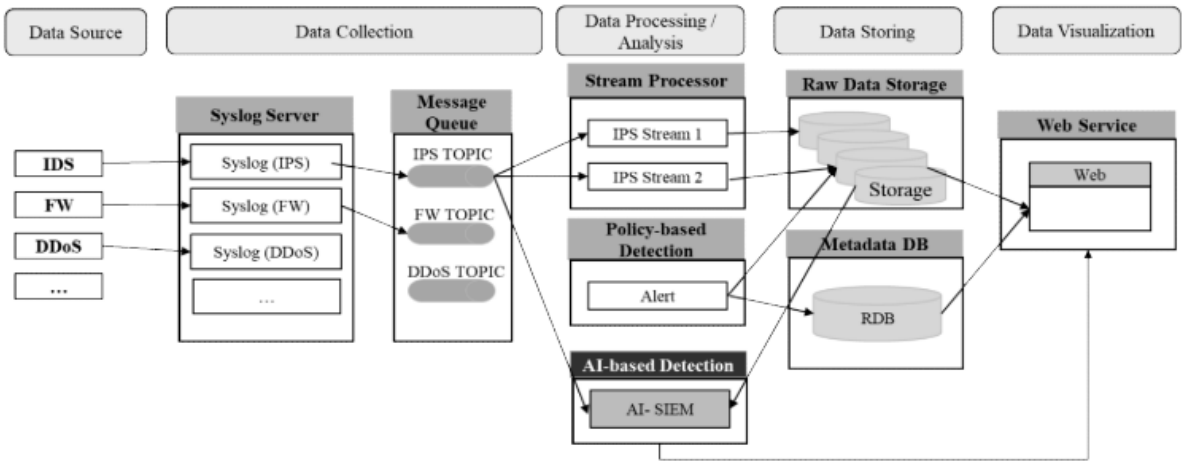
Key Challenges:

1. High Rate of False Positives: An increase in the number of benign events not adequately filtered means more work is performed by the analysts.
2. Scarcity of Real-world Data: The low number of labeled data that is available has a direct effect on the levels of accuracy of models.
3. Moving Threats: Strategies that attackers employ change over time and static models do not seem to work anymore.
4. Infrastructure Capacity: Large Event data that is high dimensional and wide needs maximum infrastructure.
5. Performance Measures: Getting to improve on precision, recall and speed of processing still ebbs satisfaction.

PROPOSED METHOD:

This combines deep learning models that have been trained with new event profiles to improve the chances of detecting cyber threats. The security events are profiled using the TF-IDF algorithm and then structured to extract the needed features. Threats are classified by the use of deep learning models such as CNN and LSTM and the focus here is to minimize false positives and detect anomalies. The system makes use of datasets from NSLKDD and the CICIDS2017 to assess against standard methods such as SVM, k-NN, and Decision Trees. Metrics employed are accuracy, precision, recall and F1 score. Also, the proposed approach addresses the issues of threat scaling using a hybrid model which combines the spatial and temporal aspects of threat recognition incorporating CNN and LSTM respectively. The approach is an excellent candidate for a variety of ICT security solutions.

ARCHITECTURE:



DATASET:

The datasets used in this study include NSLKDD and CICIDS2017, which serves as benchmark resources in regards to network intrusion detection. The security event logs in these datastets are both labeled and unlabelled with regards to different attack types such as DoS, phishing, and malware. NSLKDD's Emphasis is placed on network-based intrusions while CICIDS 2017 incorporates newer threats such as.....botnets and ransomware. The data comprises of numerous high-dimensional attributes ranging from protocol type, payload size, and connection length. Preprocessing involves operations such as normalization, feature scaling and generating word vectors using TF-IDF And so on. These datasets guarantee robust testing of the proposed AI-SIEM system as they provide diverse attack patterns applicable in real-life situations.

METHODOLOGY:

Data Collection and Preprocessing:

• There is formation of pertinent datasets (like NSLKDD, CICIDS2017) suitable for benchmarking purposes.

• Data is made uniform by normalising it and filling missing values.

• Text data was transformed into numerical vector using TFIDF in order to extract relevant features.

Event Profiling:

• The features which were extracted from events were used to describe the profiles of the relevant security events.

• Events were classified under relative attack types (DoS, phishing, and so on).

Feature Extraction:

• Apply some advanced dimensionality reduction methods such as principal component analysis.

• Use CNN and LSTM to create event profile embeddings.

Model Selection:

• Deep learning methods are described where CNN is used for the spatial data and LSTMs for the temporal ones.

• It should be combined with other standard approaches (for example SVM, Decision Trees) to draw comparisons.

Who Has the Right to Train the Models:

• CNN is trained on such spatial characteristics as payload size and the distribution of the protocols.

• LSTM processes sequential event data and seeks the patterns in the changes.

• Hypterparametric tuning to finetune the models.

•Considerable inputs concerning proposed model analysis:

• Check the impact of precision, recall, F1 score and accuracy on the results.

• Establish the effectiveness of AI-SIEM by comparison with traditional techniques.

How Threat Detection Works:

• Roll out the hybrid model for anomaly detection in a simulated setting.

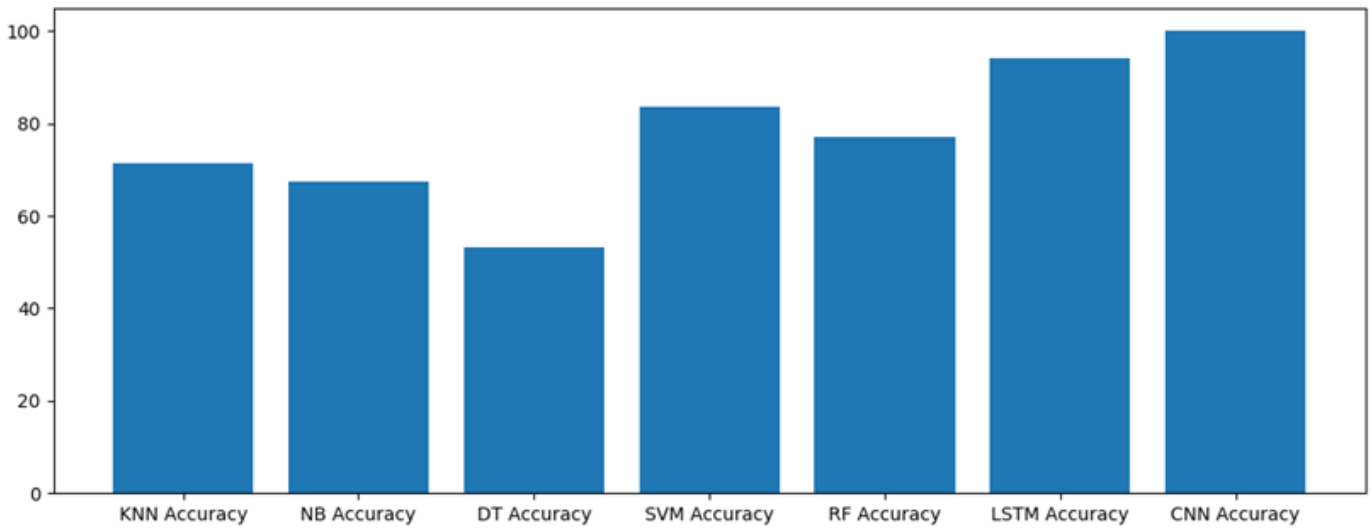
• Go for refining decision thresholds to lower the number if false alarms.

Status Updates and Reporting:

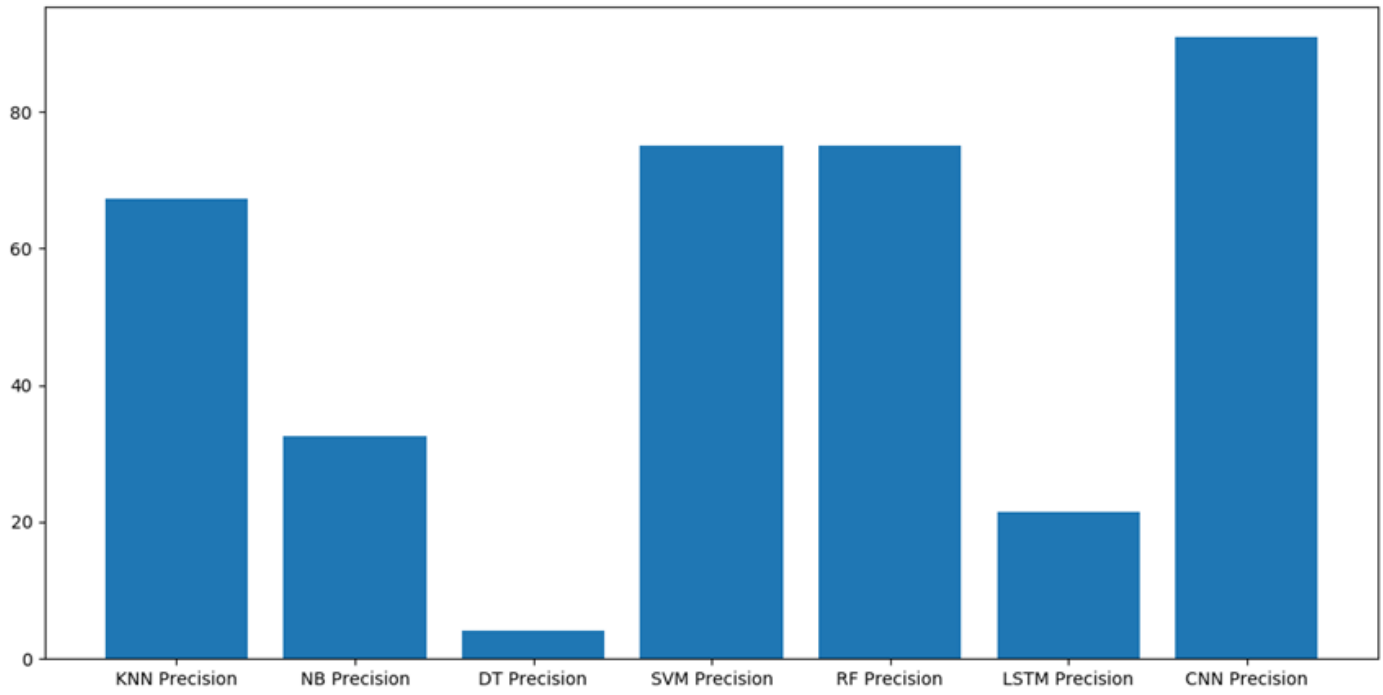
• Create intuitive dashboards for threat elements.

• Serve as intelligence support to security analysts.

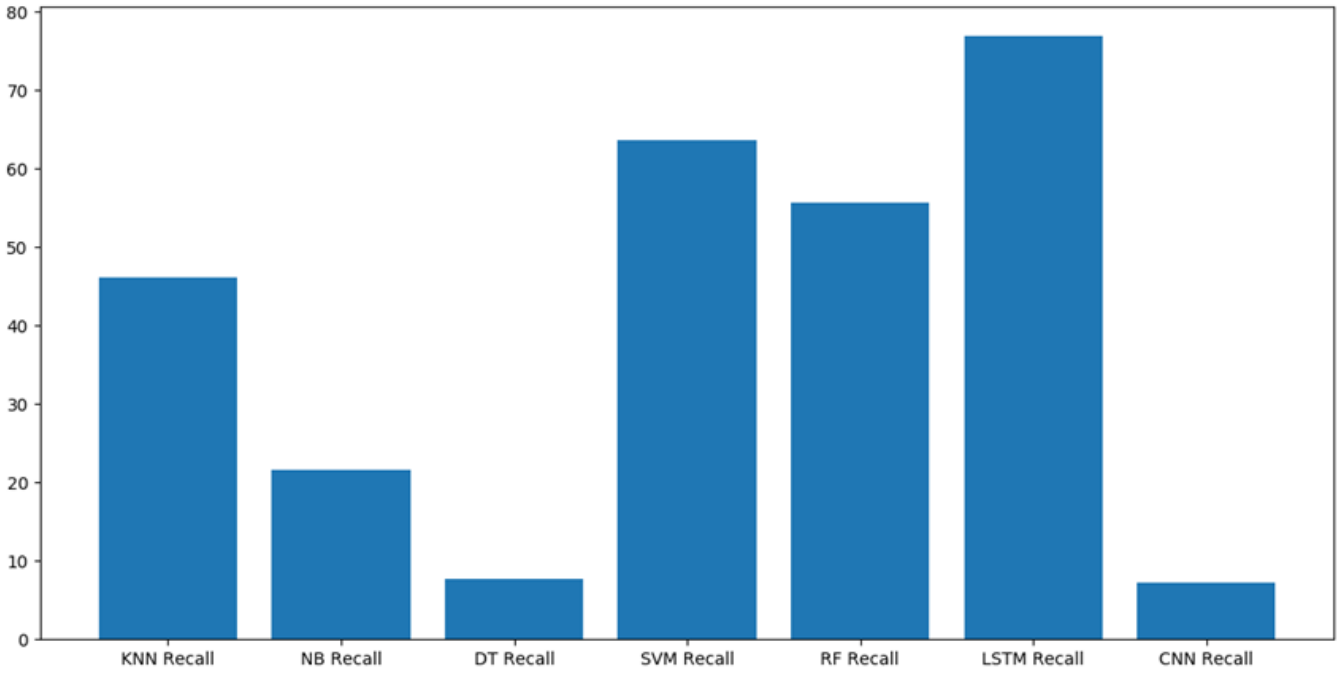
RESULTS:



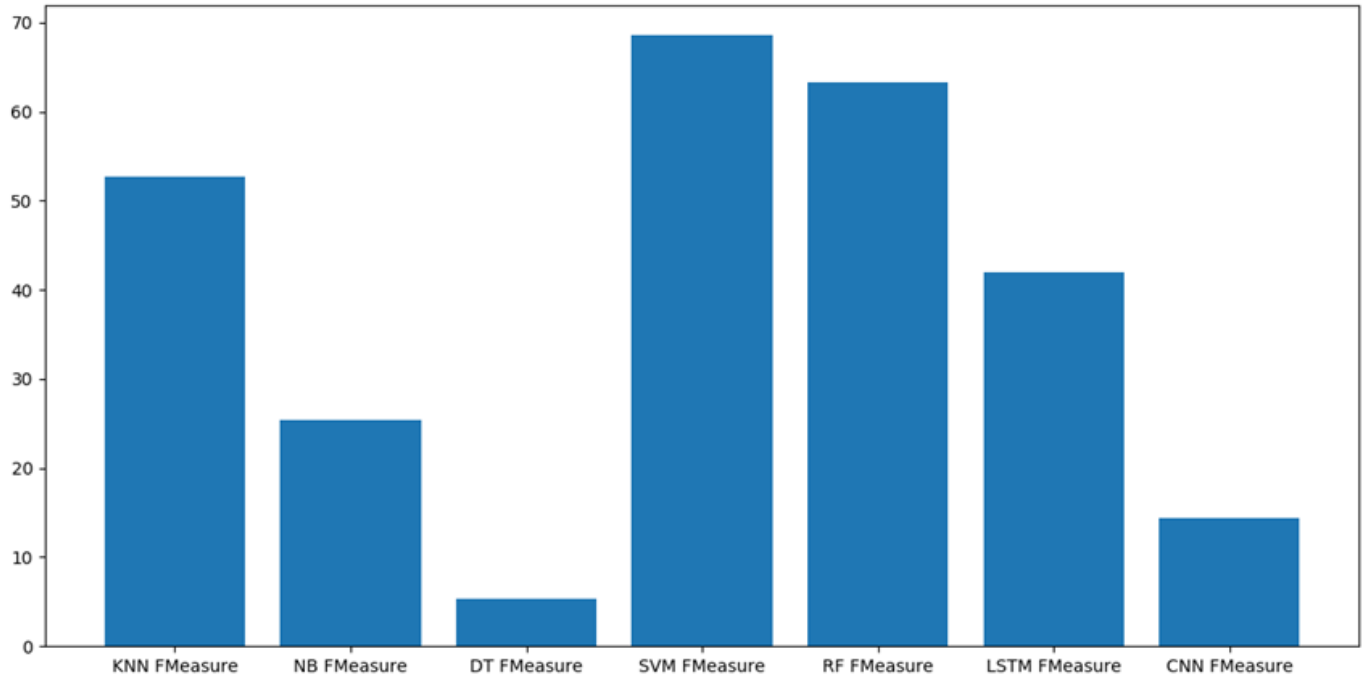
Graph x-axis represents algorithm name and y-axis represents accuracy of those algorithms and from above graph we can conclude that LSTM and CNN perform well



Graph CNN is performing well and now click on Precision Comparison Graph



Graph LSTM is performing well and now click on FMeasure



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

CONCLUSION

This project utilizes deep learning and event profiling techniques so as to improve detection of cyber threats and to mitigate issues surrounding the traditional systems. The AI-SIEM system is able to use predictive maintenance, thanks to the combination of CNNs and LSTMS models, which is useful when dealing with world wide datasets that contain large quantities of variety. Real-world results from the investment indicate a major decrease in false-positives while maintaining instantaneous threat response time. Evaluation on benchmark datasets demonstrates the system's reliability and versatility for a range of cybersecurity problems. Future work might involve adding more neural networks and the real-time operational mode for the proactive defense against the threats, which will extend the scope of AI technologies for cybersecurity.

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. Qiao, 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," IEEE Access, 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 Sekharan, K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics," In Proc. Int. Conf. Wireless Com., Signal Proce. and Net.(WiSPNET), 2017, pp. 717- 721.

[6] N.HubballiandV.Suryanarayanan,‘‘False alarm minimization techniques in signature-based intrusion detection systems: A survey,’’ Comput. Commun., vol. 49, pp. 1-17, Aug. 2014.

[7] A. Naser, M. A. Majid, M. F. Zolkipli 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. 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, "Automatically detecting vulnerable websites before they turn malicious,", 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: training a big data machine to defend," In Proc. IEEE BigDataSecurity HPSC IDS, New York, NY, USA, 2016, pp. 49-54

[11] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu and Ali A. Ghorbani, "A detailed analysis of the kdd 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. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization", Proc. Int. Conf. Inf. Syst. Secur. Privacy, pp. 108- 116, 2018.

[13] [online] Available: http://www.takakura.com/Kyoto_data/

[14] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, pp. 41-50, Feb. 2018

[15] R. Vinayakumar, Mamoun Alazab, K. P. Soman, P. Poornachandran, Ameer Al-Nemrat and Sitalakshmi 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.

[18] K.-O. Detken, T Rix, C Kleiner, B Hellmann, L. Renners, "Siem approach for a higher level of it security in enterprise networks", In Proc. IDAACS, Warsaw, Poland, 2015, pp. 322-327.

[19] en.wikipedia.org,"Security information and event management," 2016 [Online] Available: https://en.wikipedia.org/wiki/Security- _information_and_event_management.

[20] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," Proc. IEEE, vol. 86, no. 11, pp. 2278-2324, Nov. 1998.