International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET23103108

Assessment of Deep Packet Inspection System of Network traffic and Anomaly Detection

Jyoti Pandey*, Shruti Rai, Srivaramangai R
Department of Information Technology, University of Mumbai, Mumbai, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 June 2023
Published: 29 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
680-688

ABSTRACT

Deep packet SSL inspection is a process that involves decrypting and inspecting SSL encrypted network traffic in order to detect and prevent security threats. With the increasing use of SSL encryption, it has become difficult for traditional network security solutions to inspect encrypted traffic for threats. Deep packet SSL inspection addresses this problem by decrypting the SSL traffic, inspecting it for threats, and then re-encrypting it before forwarding it to its destination. This process involves the use of SSL certificates that mimic the real ones used by the servers, as well as SSL inspection rules that specify which traffic should be decrypted and inspected. Deep packet SSL inspection can be a complex and resource-intensive process, and must be performed carefully to avoid legal or ethical issues related to the interception and inspection of encrypted traffic. However, it is a powerful tool for protecting networks from security threats, and can help organizations detect and prevent attacks that would otherwise go unnoticed.

Keywords: Deep packet SSL inspection, decrypting, inspecting, SSL encrypted, network traffic.

I. INTRODUCTION

Today's communication networks are evolving rapidly. One Development of society's informatization process is the broad growth of network services, such as Internet of Things (IoT) services, Wireless Sensor Network (WSN) services, Cloud services, Wireless Sensor Multimedia Networks (WSMN) services, etc. Network traffic is rising as a result of the volume and variety of Internet services continuing to grow thanks to enhanced network technologies. This continued growth is accompanied by an increase in anomalies, such as incorrect network device setup, port scans conducted ahead of attacks, autonomously propagating resource-hogging viruses and worms, and denial-of-service (DoS) attacks that shut down network services. The management, accountability, and integrity of these systems, as well as the data's confidentiality, accessibility, and integrity, are the responsibilities of information system administrators who are in charge of the services. Additionally, they guarantee the system's normal operation and try to minimize instances of irregular behaviour and network anomalies.

A divergence from the norm is referred to as an anomaly. As a result, anything that differs from what is right or normal is referred to as anomalous. Network anomalies are deviations in the utilization of network resources accessible by network applications and online services. Hackers, careless users, hardware problems, and software defects are some of the root causes of network anomalies. The improper use of information technology has resulted in some obvious abnormalities. Although the anomalies may not show any symptoms, they can nonetheless result in failures. One of the cybersecurity fields with the highest growth right now is anomaly detection. This is due to the fact that irregularities frequently precede network attacks, which can inflict both detrimental intangible effects and monetary losses for businesses with sizable online presences. These anomalies are frequently brought on by intelligence or a "power-down" designed to further exploit found security flaws for financial gain. The IoT system as well as the whole network architecture may fail as a result of attacks and anomalies including Denial of Service, Data Type Probing, Malicious Control, Malicious Operation, Scan, Spying, and Wrong Setup. The fact that the types of anomalies might vary based on the reason, from DoS attacks (denial of service) to faulty router setups, is a key issue with anomaly identification.

Deep packet inspection (DPI) is a technique used to analyze and monitor network traffic at the packet level. DPI involves the inspection of the content of packets, as well as their header information. This technique enables the detection of a wide range of security threats, including malware, viruses, and other types of attacks. DPI can be used in conjunction with intrusion detection systems (IDS) and intrusion prevention systems (IPS) to provide a comprehensive approach to network security. IDS systems monitor network traffic for signs of attacks, while IPS systems can actively block or prevent malicious traffic from entering the network. SSL (Secure Sockets Layer) is a protocol used to encrypt data transmitted over the internet. It is commonly used to secure sensitive data such as financial transactions, login credentials, and personal information. SSL works by encrypting the data at the sender's end and decrypting it at the receiver's end. However, this encryption can also be used to hide malicious traffic, making it difficult for traditional security solutions to detect and prevent security threats.

Deep packet SSL inspection (DPI-SSL) is a specific type of DPI that focuses on inspecting SSL- encrypted traffic. As mentioned earlier, SSL encryption can be used to hide malicious traffic, making it difficult for traditional security solutions to detect and prevent security threats. DPI-SSL overcomes this challenge by decrypting the SSL traffic and inspecting it for threats. IDS and IPS functionality can be incorporated into DPI-SSL systems to enable the detection and prevention of a variety of security risks. The system has the ability to be set up to watch SSL traffic and detect potential security risks like malware or unauthorized access attempts. The system can then take action if a threat is identified to stop it from harming the network. DPI-SSL overcomes this challenge by decrypting the SSL traffic and inspecting it for threats. This process involves the use of SSL certificates that mimic the real ones used by the servers, as well as SSL inspection rules that specify which traffic should be decrypted and inspected. The decrypted traffic can then be analyzed for malware, viruses, spam, and other security threats. Once any threats have been detected, the traffic can be blocked or quarantined to prevent further damage. While DPI-SSL is a powerful tool for protecting networks from security threats, it can also raise concerns about privacy and data protection. The interception and inspection of encrypted traffic must be performed carefully and transparently to avoid legal or ethical issues. Nevertheless, DPI- SSL remains an essential technique for ensuring network security in today's highly connected world.

In summary, DPI-SSL is a powerful technique for ensuring network security by monitoring and analyzing SSL-encrypted traffic. By incorporating IDS and IPS functionality, DPI-SSL systems can provide a comprehensive approach to network security, enabling the detection and prevention of a wide range of security threats.

II. LITERATURE SURVEY

In this section, we present the current state of the study on the information network anomaly detection approaches Md. Ahsanul Kabir, and Xiao luo [1] examines and compare the performance of four unsupervised learning algorithms: K-Means and Self Organizing Maps (SOM), deep auto encoding Gaussian mixture model (DAGMM), and adversarially learned anomaly detection (ALAD) in the direction of network flow-based anomaly detection. We investigate various neural network setups and learning algorithm parameters, accordingly. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho [2] uses Software Defined Networking by applying a deep learning approach for flow-based anomaly detection in an SDN environment and building a Deep Neural Network (DNN) model for an intrusion detection system and train the model with the NSL-KDD Dataset. In this research, six basic features (that can be easily obtained in an SDN environment) taken from the forty-one features of NSL-KDD Dataset. S. Potluri and C. Diedrich [3] apply Deep Neural Network (DNN) to efficiently and quickly comb through the network traffic and to find the anomalies in the network data. The training time is calculated, and the efficiency of the detection mechanism is examined using the NSL-KDD dataset. D. Kwon, K. Natarajan, S. C. Suh, H. Kim, and J. Kim[4] evaluated three deep learning models, the Fully Connected Network (FCN), Variational Auto Encoder (VAE), and Sequence to Sequence model with Long Short-Term Memory (Seq2Seq-LSTM), and Convolution Neural Networks (CNNs) for detecting network anomalies by setting three simple CNN models with different internal depths (shallow CNN, moderate CNN, and deep CNN) to see the impact of the depth on the performance. Set up three simple CNN models with different internal depths (shallow CNN, moderate CNN, and deep CNN) to see the impact of the depth on the performance. Kim, J. Kim, H. L. T. Thu, and H. Kim [5] construct an IDS model with a deep learning approach, apply the Long Short Term Memory (LSTM) architecture to a recurrent neural network (RNN), and train the IDS model using the KDD Cup 1999 dataset. Through the performance test, confirm that the deep learning approach is effective for IDS. B.Stewart, Luis Rosa, Leaodros A. Maglaras, Taigo J. Cruz, Mohamed Amine Ferrag, Paulo Simones, and Helge Janicke [6] examines how modifications to a supervisory control and data acquisition (SCADA) system's network design affect the effectiveness of an Intrusion Detection System (IDS) based on a single-class support vector machine (OCSVM). The article also suggests an adaptive system that may deal with such changes and function in actual-world circumstances. Traces from a hybrid ICS testbed with a dynamic topology are used to gauge how well the proposed adaptive IDS performs. C. Yin, Y. Zhu, J. Fei, and X. He [7] investigate the model's performance in binary classification and multiclass classification, as well as the effects of the number of neurons and varying learning rates. On the benchmark data set, compare it to those of J48, artificial neural networks, random forests, support vector machines, and other machine learning techniques and demonstrate that RNN-IDS performs better than typical machine learning classification methods in both binary and multiclass classification, and that it is particularly well suited for developing a classification model with high accuracy. The RNN-IDS model enhances intrusion detection accuracy and offers a fresh approach to intrusion detection research. Felix Iglesias and Tanja Zseby [8] proposed a multi- stage feature selection strategy using filters and stepwise regression wrappers to handle the feature selection issue for network traffic based anomaly detection. Analysis is based on 41 widely- adopted traffic features that are presented in several commonly used traffic data sets. Benjamin J. Radford, Leonardo M. Apolonio, Antonio J. Trias, and

Jim A. Simpson [9] demonstrate how a recurrent neural network may be used to detect anomalous network traffic and learn a model to represent sequences of communications between computers. LSTM cell recurrent neural networks (RNN) can be used to represent the intricate linkages and subtleties of this language. The communications between two IPs are then predicted using the language model, and the prediction error is utilised as a gauge of how typical or atypical the observed communications are. A language model may recognise patterns of network activity that deviate from the model by learning a model that is unique to each network while also being generalised to normal computer- to-computer traffic inside and outside the network. Raghavendra Chalapathy and Sanjay Chawla [10] provide an organised and thorough review of research methods in deep learning- based anomaly detection. Divided cutting-edge research methods into many groups based on the underlying assumptions and methods used and described the fundamental method for distinguishing between normal and abnormal behaviour for each category, as well as its variations and fundamental presuppositions. Saika Das, Mohammad Ashrafuzzaman, Fededrick T. Sheldon, and Sajjan Shiva [11] suggests an intrusion detection system (NLPIDS) that makes use of machine learning based on ensembles and natural language processing. The suggested NLPIDS transforms vectors of HTTP requests from natural language into supervised and ensemble-based machine learning models. Then, to identify unusual traffic, the trained models are put to action. Using HTTP DATASET CSIC 2010, verified the methodology. The results demonstrate the NLPIDS' effectiveness by generating a higher F1-score (0.999) and very few false alarms (0.007) when compared to previous techniques. Qian Ma, Cong Sun, and Baojiang Cui [12] suggested the SVM-C model as a novel model for the detection of anomalies in network data. Through the use of statistical principles and linear projection, the URLs in the network traffic log are converted into feature vectors. The acquired feature vectors are categorised as normal or abnormal using a support vector machine (SVM) classifier. An optimization model is built to train the feature extraction method and traffic classifier's parameters using the concepts of SVM and clustering. Mahdi Rabbani ,Yongli Wang, Reza Khoshkangini Hamed Jelodar, Ruxin Zhao, Sajjad Bagheri Baba Ahmadi and Seyedvayallah Ayobi [13] provides a thorough analysis of the various features of anomaly-based network intrusion detection systems (NIDSs). Furthermore, current harmful actions in network systems as well as crucial characteristics of intrusion detection systems are examined. The current survey explains key NADSs processes such pre- processing, feature extraction, and the detection and identification of dangerous behaviour. Varun Chandola, Arindham Banerjee, and Vipin Kumar [14] distinguish between typical and abnormal conduct. These presumptions can be used as guides to determine whether a particular technique is effective in a given area when applied to it. A fundamental anomaly detection method is given for each category, followed by an explanation of how the various extant methods fall under that category and how they differ from the basic method. Ali Bou Nassif, Manar Abu Talib, Qassim Nasir, and Fatima Mohamad Dokalbab [15] undertake a Systematic Literature Review (SLR) that examines ML models that identify anomalies in their applications from four perspectives: the classification of anomaly detection, the applications of anomaly detection, ML methodologies, and performance measures for ML models. Fadi Salo, Mohammadnoor Injadat, Ali Bou Nassif, and Aleksander Essex [16] classify the fields of data mining and intrusion detection systems, providing a systematic treatment of methodologies and techniques, use a criterion- based approach to select 95 relevant articles from 2007 to 2017, identified 19 different data mining techniques used for intrusion detection, encompasses rich information for future research based on the strengths and weaknesses of these technique and also noticed a research gap in establishing the relationship between data mining and intrusion detection systems. Yang Yu, Jun Long and Zhiping Cai [17] proposed a novel network intrusion model and test it on two fresh intrusion detection datasets by stacking dilated convolutional autoencoders, Several tests were performed to see whether our strategy was effective. The results of the comparative experiments show that the suggested model can reach noticeably high performance that satisfies the need of high accuracy and adaptability of network intrusion detection systems (NIDSs). Gagandeep Kaur, Vikas Saxena J.P. Gupta [18] explains the main techniques known in the field of Statistical based and Wavelet based anomaly detection approaches and focuses on the role of data traffic visualization tools in network traffic anomaly detection Duong Ha Nguyen, Dang Hai Hoang [19] offers a semi-supervised model based on a combination of Mahalanobis distance and principal component analysis for the purpose of detecting network traffic anomalies. It also includes some improved detection techniques and an experiment with a clustering technique with the right features to reduce noise in training data. Anomaly detection and signature-based detection systems are combined in this strategy. Basant Agarwal, and Namita Mittal [20] contrasts Support Vector Machine (SVM) and an anomaly traffic detection system based on the entropy of network features. Additionally, a hybrid approach that combines the entropy of network characteristics and the support vector machine is contrasted with separate approaches. The approaches are assessed using the DARPA Intrusion Detection Evaluation dataset. It has been demonstrated that entropy- based detection techniques are more effective than support vector machine-based detection systems at detecting network anomalies. Paul Bardford, Jeffrey Kline, David Plonka, and Amos Ron [21] report the findings from a signal analysis of the four different types of network traffic anomalies: attacks, flash crowds, measurement failures, and outages. This study's data consists of IP flow and SNMP measurements that were gathered over a six-month period at the border router of a large university. It demonstrates that detecting a sharp increase in the local variance of the filtered data is an effective method of exposing anomalies. It also evaluates traffic anomaly signals at various points within a network based on topological distance from the anomaly source or destination, demonstrating that anomalies can be exposed effectively even when aggravating factors are present. Yu Gu, Andrew McCallum, Don Towsley [22] create a behaviour-based anomaly detection technique that assesses the distribution of network traffic against a baseline to identify network anomalies. A quick and flexible method for determining the baseline distribution is the Maximum Entropy methodology, which also gives the network administrator a multi-dimensional picture of the network traffic. By calculating a measure related to the relative entropy of the network traffic under observation with respect to the baseline distribution, it is possible to discern anomalies that modify the traffic abruptly or gradually. Additionally, the approach offers details on the kind of abnormality found. Monowar H. Bhuyan, D. K. Bhattacharya. And J. K. Kalita [23] provide a structured and comprehensive overview of various facets of network anomaly detection so that a researcher can become quickly familiar with every aspect of network anomaly detection. Based on the underlying computational methodologies employed, classify the current network anomaly detection methods and systems and define brief outline, and contrast numerous techniques and systems for detecting network anomalies. It also go over network defence technologies and datasets that researchers interested in network anomaly detection might employ. ChoXuan Do, Nguyen Quang Dam, and Nguyen Tung Lam [24] suggest two key ways to improve: improving the characteristics and the detecting algorithm. These two optimization techniques both attempt to shorten analysis and detection times while increasing accuracy. As a result, the supervised classification algorithm Random Forest was employed for the detection approach. Because the findings of the Random Forest algorithm are far superior to those of some other detection algorithms on all measures, it is absolutely correct for detecting deviant behaviour. Utilizing data dimensional reduction approaches such information gain, principal component analysis, and correlation coefficient method is suggested for the feature optimization solution. Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Koji Nakao [25] offer a new anomaly detection technique to automatically modify and optimise parameter values without predefining them. The suggested technique was tested using actual traffic data gathered from Kyoto University honeypots. The results of the experiments demonstrate that the proposed strategy performs better than the original. Edin Citaku [26] demonstrates the value of machine learning as a tool for generating an accurate understanding of what constitutes normal or abnormal behaviour in a network system. It also examines the most popular machine learning applications for anomaly detection and describes how these applications were used in recent research. Haiyan Wang [27] suggest a hybrid approach for network traffic forecasting and anomaly identification. The original network traffic data is broken down specifically into high- frequency and low-frequency components. Then, for prediction, the non-linear Relevance Vector Machine (RVM) and ARMA (Auto Regressive Moving Average) models are used, respectively. A self-adaptive threshold method based on the Central Limit Theorem (LCT) is then developed for anomaly detection after combining the predictions. Hemant Sengar, Xinyuan Wang, Haining Wang, Duminda Wijesekera, and Sushil Jajodia [28] create a framework for behavioural distance-based anomaly identification that can analyse online traffic and pr esent horizontal and vertical distance measures between different traffic aspects (in the traffic data streams in order to build precise online traffic profiles. The proposed approach has four key benefits: (1) it processes online traffic data effectively and simply; (2) it facilitates protocol behavioural analysis without maintaining per-flow state; (3) it is scalable to high speed traffic links due to the aggregation; and (4) it is capable of accurate online anomaly detection using different combinations of packet features and measuring distances between them. Nana K. Ampah, Cajetan M. Akujuobi, Mathew N.O. Sadiku and Shumon Alam [29] discuss strategies used by IDSs are anomaly- and signature-based techniques. The statistical and predictive pattern generating approaches serve as the foundation for this novel IDS technique. Using signature-based and anomaly detection methods, this IDS will find both known and undiscovered assaults. Kai Steverson; Caleb Carlin; Jonathan Mullin; Metin Ahiskali [30] combines deep learning and natural language processing to suggest ways to detect cyberattacks in Windows Event Logs. Data is gathered through a network simulation that mimics a corporate network. A spear phishing email and the endless blue exploit are used in a cyber-attack on the network to spread botnet software. The transformer model and self- supervised training are used to create a machine learning anomaly detection technique. With almost perfect accuracy and recall, the model is able to identify both the infected devices and the timing of the attack.

III.CONCLUSION

In this paper previous Network traffic techniques has been observed and discussed and a new e network traffic analysing technique has been prososed. Deep packet inspection (DPI) is a technique that allows for the analysis and monitoring of network traffic at the packet level by inspecting both the content of packets and their header information. DPI-SSL is a type of DPI that specializes in inspecting SSL-encrypted traffic. SSL encryption can be used to hide malicious traffic from traditional security solutions, making it challenging to detect and prevent security threats. DPI-SSL addresses this issue by decrypting SSL traffic, examining it for security risks and then re- encrypting it before sending it to its intended destination.

IV. REFERENCES

[1]. Kabir, Md Ahsanul, and Xiao Luo. "Unsupervised learning for network flow based anomaly detection in the era of deep learning." In 2020 IEEE Sixth International Conference on Big Data Computing Service and Applications (BigDataService), pp. 165-168. IEEE, 2020.

[2]. Tang, Tuan A., Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, and Mounir Ghogho. "Deep learning approach for network intrusion detection in software defined networking." In 2016 international conference on wireless networks and mobile communications (WINCOM), pp. 258-263. IEEE, 2016.

[3]. Potluri, Sasanka, and Christian Diedrich. "Accelerated deep neural networks for enhanced intrusion detection system." In 2016 IEEE 21st international conference on emerging technologies and factory automation (ETFA), pp. 1-8. IEEE, 2016.

[4]. D. Kwon, K. Natarajan, S. C. Suh, H. Kim, and J. Kim, "An empirical study on network anomaly detection using convolutional neural networks," in 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018, pp. 1595–1598

[5]. Kim, Jihyun, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim. "Long short term memory recurrent neural network classifier for intrusion detection." In 2016 international conference on platform technology and service (PlatCon), pp. 1-5. IEEE, 2016.

[6]. Stewart, Barnaby, Luis Rosa, Leandros A. Maglaras, Tiago J. Cruz, Mohamed Amine Ferrag, Paulo Simoes, and Helge Janicke. "A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes." EAI Endorsed Transactions on Industrial Networks and Intelligent Systems 4, no. 10 (2017).

[7]. C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," Ieee Access, vol. 5, pp. 21 954–21 961, 2017.

[8]. Iglesias, F., Zseby, T. Analysis of network traffic features for anomaly detection. Mach Learn 101, 59–84 (2015). https://doi.org/10.1007/s10994-014-5473-9 .

[9]. Benjamin J. Radford, Leonardo M. Apolonio, Antonio J. Trias, and Jim A. Simpson, "Network Traffic Anomaly detection using Recurrent Neural Network", 2018 arXiv:1803.10769.

[10]. Raghavendra Chalapathy and Sanjay Chawla, "Deep Learning for Anomaly Detection: A Survey" 2019. arXv:1901.03407v2.

[11]. S. Das, M. Ashrafuzzaman, F. T. Sheldon and S. Shiva, "Network Intrusion Detection using Natural Language Processing and Ensemble Machine Learning," 2020 IEEE Symposium Series on Computational Intelligence (SSCI), Canberra, ACT, Australia, 2020, pp. 829-835, doi: 10.1109/SSCI47803.2020.9308268

[12]. Ma, Qian & Sun, Cong & Cui, Baojiang & Jin, Xiaohui. (2021). A Novel Model for Anomaly Detection in Network Traffic Based on Kernel Support Vector Machine. Computers & Security. 104. 102215. 10.1016/j.cose.2021.102215.

[13]. Rabbani, M.; Wang, Y.; Khoshkangini, R.; Jelodar, H.; Zhao, R.; Bagheri Baba Ahmadi, S.; Ayobi, S. A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies. Entropy 2021, 23, 529. https://doi.org/10.3390/e23050529

[14]. Chandola, Varun & Banerjee, Arindam & Kumar, Vipin. (2009). Anomaly Detection: A Survey. ACM Comput. Surv 41.10.1145/1541880.1541882.

[15]. A. B. Nassif, M. A. Talib, Q. Nasir and F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," in IEEE Access, vol. 9, pp. 78658-78700, 2021, doi: 10.1109/ACCESS.2021.3083060.

[16]. F. Salo, M. Injadat, A. B. Nassif, A. Shami and A. Essex, "Data Mining Techniques in Intrusion Detection Systems: A Systematic Literature Review," in IEEE Access, vol. 6, pp. 56046-56058, 2018, doi:10.1109/ACCESS.2018.2872784

[17]. Yu, Yang & Long, Jun & Cai, Zhiping. (2017). Network Intrusion Detection through Stacking Dilated Convolutional Autoencoders. Security and Communication Networks. 2017. 1-10. 10.1155/2017/4184196

[18]. G. Kaur, V. Saxena and J. P. Gupta, "Anomaly Detection in network traffic and role of wavelets," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 2010, pp. V7-46-V7-51, doi: 10.1109/ICCET.2010.5485392.

[19]. N. H. Duong and H. Dang Hai, "A model for network traffic anomaly detection," 2016 18th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 2016, pp. 644-650, doi: 10.1109/ICACT.2016.7423587.

[20]. Agarwal, Basant & Mittal, Namita. (2012). Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques. Procedia Technology. 6.10.1016/j.protcy.2012.10.121.

[21]. Paul Barford, Jeffery Kline, David Plonka, and Amos Ron. 2002. A signal analysis of network traffic anomalies. In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment (IMW '02). Association for Computing Machinery, NewYork,NY,USA, 71–82. https://doi.org/10.1145/637201.637210

[22]. Gu, Yu & Mccallum, Andrew & Towsley, Donald. (2005). Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation 345-350. 10.1145/1330107.1330148.

[23]. M. H. Bhuyan, D. K. Bhattacharyya and J.K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303-336, First Quarter 2014, doi: 10.1109/SURV.2013.052213.00046.

[24]. Do, ChoXuan & Dam, Nguyen & Lam, Nguyen. (2021). Optimization of network traffic anomaly detection using machine learning. International Journal of Electrical and Computer Engineering(IJECE). 11.2360.10.11591/ijece.v11i3.pp2360-2370.

[25]. Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Koji Nakao, ”Toward a more practical unsupervised anomaly detection system”,Information Sciences, Volume 231,2013, Pages 4-14, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2011.08.011 .

[26]. Edin Citaku, “Use case study on machine earning for network anomaly detection” in Seminar Innovative Internet Technologies and Mobile Communications Chair of Network Architectures and Services Departments of Informatics, Technical University of Munich,2018.

[27]. Wang, Haiyan. (2015). Anomaly Detection of Network Traffic Based on Prediction and Self-Adaptive Threshold. International Journal of Future Generation Communication and Networking. 8. 205-214. 10.14257/ijfgcn.2015.8.6.20.

[28]. Hemant Sengar, H., Wang, X., Wang, H., Wijesekera, D., & Jajodia, S. (2009). Online detection of network traffic anomalies using behavioral distance. 2009 17th International Workshop on Quality of Service, 1-9.

[29]. Nana K. Ampah, Cajetan M. Akujuobi, Mathew N.O. Sadiku and Shumon Alam, “An intrusion detection technique based on continuous binary communication channels”, November 16, 2011 pp 174-180, tps://doi.org/10.1504/IJSN.2011.043674.

[30]. K. Steverson, C. Carlin, J. Mullin and M. Ahiskali, "Cyber Intrusion Detection using Natural Language Processing on Windows Event Logs," 2021 International Conference on

Military Communication and Information Systems (ICMCIS), The Hague, Netherlands, 2021, pp. 1-7, doi: 10.1109/ICMCIS52405.2021.9486307.

Cite this article as :

Jyoti Pandey, Shruti Rai, Srivaramangai R, "Assessment of Deep Packet Inspection System of Network traffic and Anomaly Detection", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 3, pp. 680-688, May-June 2023. Available at doi : https://doi.org/10.32628/IJSRSET23103108
Journal URL : https://ijsrset.com/IJSRSET23103108