Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 22, No. 3, July 2023, pp. 665∼672
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v22i3.3089

Data Exfiltration Anomaly Detection on Enterprise Networks using Deep Packet Inspection

Jelita Asian, Dimas Erlangga, Media Ayu
Nusa Putra University, Sukabumi, Indonesia

Article Info

Article history:

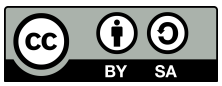
Received May 10, 2023
Revised July 5, 2023
Accepted July 20, 2023

Keywords:

Anomaly Detection
Data Exfiltration
Deep Packet Inspection
Enterprise Networks

ABSTRACT

Advanced persistent threats (APT) are threat actors with the advanced Technique, Tactic and Procedure (TTP) to gain covert control of the computer network for a long period of time. These threat actors are the highest cyber attack risk factor for enterprise companies and governments. A successful attack by the APT threat Actors has the capabilities to do physical damage. APT groups are typically state-sponsored and are considered the most effective and skilled cyber attackers. The final goal for the APT Attack is to exfiltrate victims data or sabotage system. This aim of this research is to exercise multiple Machine Learning Approach such as k-Nearest Neighbors and H20 Deep Learning Model and also employ Deep Packet Inspection on enterprise network traffic dataset in order to identify suitable approaches to detect data exfiltration by APT threat Actors. This study shows that combining machine learning techniques with Deep Packet Inspection significantly improves the detection of data exfiltration attempts by Advanced Persistent Threat (APT) actors. The findings suggest that this approach can enhance anomaly detection systems, bolstering the cybersecurity defenses of enterprises. Consequently, the research implications could lead to developing more robust strategies against sophisticated and covert cyber threats posed by APTs.



Corresponding Author:

Jelita Asian
School of Computer Science,
Nusa Putra University, Sukabumi, Indonesia,
Email: jelita.asian@nusaputra.ac.id

How to Cite:
J. Asian, D. Erlanggga, and M. Ayu "Data Exfiltration Anomaly Detection on Enterprise Networks using Deep Packet Inspection", *MATRIK: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer*, 22.3. pp. 665-672, 2023.

1. INTRODUCTION

Advanced Persistent Threat (APT) is often described as a cyber security threat that is highly organized and well-funded by organizations to sabotage or conduct cyber espionage to extract critical information from its target. Using numerous customized attack vectors, APT groups organize attacks into multiple stages. They use obfuscation techniques to evade security personnel deployed in their victims' networks. APT could lead to the potential loss of critical data by espionage or sabotage efforts. The APT attack consists of five main phases: Reconnaissance, Foothold Establishment, Lateral Movement, Data Exfiltration, and Post-Exfiltration [1]. In 2021, the National Cyber and Cypher Agency (BSSN) detected about 1,6 billion cyber attacks on numerous organizations and government entities in Indonesia. Most of these attacks consist of website defacement, data breach, installation of malware, and APT Attacks [2]. This shows that organizations and government entities are not safe from APT attacks, which could potentially lead to the theft or destruction of sensitive and critical data.

APTs are threat actors who employ Advanced Techniques, Tactics, and Procedures (TTP) to gain covert control of computer networks for a long period of time. These threat actors are the highest form of cyber attack for enterprise companies and governments. A successful attack by the APT threat actor can cause physical damage. APT groups are typically state-sponsored and considered to be the most effective and skilled cyber attackers. This has become a challenge for network defenders and security experts because APT attacks are hard to detect by common Intrusion Detection Systems (IDS). IDS alerts are often overloaded by benign network traffic (false positives). On the other hand, reducing false positives can cause an increased rate of attacks marked as false negatives [3]. This situation could allow attackers to go through the network undetected. In an APT attack, attackers could use various methods to intrude, including Zero Day, in which attackers identify the weaknesses of a company or an organization and use them to damage the systems [1]; targeted Phishing, where attackers use infected emails that contain malware to intrude the systems [1]. In an APT attack, attackers often try to find the codes of their target systems and the executed programs at the beginning of the task to intrude into the system of their victims.

One of the challenges associated with APT attacks is a lack of a high-precision, real-time detection system. The other challenge is stopping the attacker from analyzing the victim system using structured models placed in the target system undetected for a long time [4]. Some of the methods to detect APT attacks are detection models based on machine learning algorithms, including linear support vector machine, Quadratic SVM, Cubic SVM, Fine Gaussian SVM, Medium Gaussian SVM, Coarse Gaussian SVM [5] as a subset of SVM methods as well as decision trees like Complex tree, Medium tree, and Simple tree [6]. Detection models based on mathematical models, such as the Hidden Markov Model [7], are also used. Several known methods mentioned before could potentially become appropriate detection methods for APT attacks; however, they are harder to use for real-time detection. These methods lack precision. The possibilities for false negatives and false positives are also high, which reflects the ineffectiveness. Detecting new attack patterns is also a problem that these previous methods are still unable to stop. Moreover, the lack of proper processes on the dataset of the attacks in these methods makes the validity questionable.

Therefore, we decided to exercise several Machine Learning methods, such as k-Nearest Neighbors and the H20 Deep Learning model, while using Deep Packet Inspection on Enterprise Networks to identify the exact approach to detecting the data exfiltration phase by the APT Threat Actors. This work uses an Enterprise Network Dataset called END-22, extracted from Deep Packet Inspection during a week, with an APT attack signature and large packets transferred. Furthermore, this work is followed by combining several methods such as Data Collection, Preprocessing, Classifiers using k-Nearest Neighbors and the H20 Deep Learning Model and Evaluation to determine Accuracy, False Positive Rate (FPR), True Positive Rate (TPR), Precision, Sensitivity, and F1-Score. This work collects about 84 strings of network logs from Deep Packet Inspection on Enterprise Networks. The main contributions of this article are as follows: (1). Collecting END-22 Dataset that contains about 84 strings of network logs from Deep Packet Inspection on Enterprise Networks. (2). Improving Data Exfiltration Anomaly Detection using k-Nearest Neighbors and H20 Deep Learning Model in order to avoid False Negatives and Detects Data Exfiltration phase in APT Attacks more accurate. The detection methods of APT attacks that have been introduced up to now have disadvantages, such as a high rate of false detection of the attacks and lack of real-time detection. Since APT attacks use secret and intelligent techniques and can stay in the system for months, traditional intrusion detection systems cannot detect these attacks because they are usually based on patterns or signatures and need third-party applications to detect APT [8]. Earlier APT attack detection methods using different criteria are mentioned in the following paragraphs. Among these methods, better detection methods usually use machine learning. Javad et al. [9] conducted Early Detection of The Advanced Persistent Threat Attack Using Performance Analysis of Machine Learning Methods such as C5.0 decision tree, Bayesian network, and deep neural network used for timely detection and classification of APT-attacks on the NSL-KDD dataset. As a result, the accuracy (ACC) of the C5.0 decision tree, Bayesian network, and 6-layer deep learning models are 95.64%, 88.37%, and 98.85%, respectively. Another important criterion for measure is the FPR. The FPR values for the C5.0 decision tree, Bayesian network, and 6-layer deep learning models are 2.56, 10.47, and 1.13. Other criteria such as sensitivity, specificity, accuracy, false negative rate, and F-measure are also investigated for the models. The experimental results show that the deep learning model with

automatic multi-layered extraction of features has the best performance for the timely detection of an APT attack as compared to other classification models.

Allard Dijk [10] implemented a CICFlowmeter in a Python environment as a new method to incorporate payload data for deep packet inspection with artificial intelligence. The research also uses several artificial intelligence models such as One Class State Vector Machine, Stacked Auto Encoder, Recurrent Neural Network, and APT-2020 Dataset to detect anomalous traffic for all APT Stages, including Data Exfiltration Stages. This research improves on models of data inspection on the Data Exfiltration stage and incorporates and exploits the context of packets in traffic analysis, which is important to detect APT behavior in computer networks. Hwang et al. [11] conducted research for early network traffic anomaly detection using an unsupervised model (autoencoder) trained with the output data of targets to build the profile of benign traffic and then judged whether the traffic in the examined flows was abnormal. They also used a CNN-based deep learning approach for auto-learning the traffic features and profiling traffic directly from the raw traffic with only a few first packets per flow. The evaluation of the datasets from multiple sources shows that D-PACK can achieve nearly 100% accuracy and precision in detecting malicious packets. Design on packet-based deep learning classification and detection provided promising valuable information. It inspired the research community to overcome the remaining challenges, particularly in speeding up online DL-based anomaly detection. D-PACK could detect malicious traffic with nearly 100% accuracy and less than 1% FNR and FPR. D-PACK only needs to examine two packets from each flow and 80 bytes from each packet.

Bibal et al. [12] conducted performance analysis using a hybrid method with DPI, Pattern Matching (PM), and Machine Learning (ML) techniques for Deep Packet Inspection in Firewalls. Ten ML algorithms are employed for data classification. Meanwhile, DPI uses Boyer-Moore-Horspool (BMHP) pattern-matching algorithms. This method is evaluated in a sequential and parallel manner, and it is customized for identifying the fuzzy, impersonation Denial of Service (DoS)-based attacks. The method is analyzed in different dimensions, such as the performance of ML methods and the role of DPI in attack identification, including the pattern matching efficiency. The method identified that the BMHP algorithm consumes the least time and memory, about 0.0028 sec and 125.4 Mib, respectively. Meanwhile, SVM has an accuracy of 99.91% with the least time and memory consumed, about 18.185 sec and 303.5 MiB, respectively.

Velea et al. [13] used Shallow Packet Inspection and Parallel K-means data Clustering to conduct network traffic anomaly detection. The method provides an overview of events on the network and visualization of anomalies, which could help track down security vulnerabilities and adjust network policies. This work adopts K-Means Clustering using multiple parallel APIs to provide detection of anomalous behavior in network traffic without performing deep packet inspection and using Multiple Frameworks for data clusterization, such as CUDA, OpenCL, and OpenMP. The research introduces K-Means to create data clusterization that allows users to encapsulate extracted data smaller and faster without reducing detection accuracy. This method could provide the quickest way to classify data and perform well in parallel environments. Statistical methods have also been used to detect APT attacks. The hidden Markov model is one of these methods. Ghafir et al. [7] have developed a system that could effectively predict and detect APT attacks. The system consists of two parts. The first one examines the correlation of the warnings, and the second uses the Markov model to decrypt the attack and count the warnings or steps of the APT attack. The system could estimate the sequence of attack steps with an accuracy of 91.80%. Compared to previous studies, this research introduces a novel approach by combining machine learning techniques with Deep Packet Inspection (DPI) to enhance the detection of data exfiltration attempts by Advanced Persistent Threat (APT) actors. Unlike earlier methods that either focused on machine learning models or DPI separately, this study integrates both to address the limitations of high false detection rates and lack of real-time detection. Additionally, this research goes beyond traditional intrusion detection systems by employing a multi-layered analysis of network traffic, which significantly improves the detection accuracy and reduces false positives in identifying covert APT activities. The benefit of this study lies in its potential to significantly improve the cybersecurity posture of enterprises by providing a more accurate and real-time detection system for APT attacks. By leveraging the strengths of both machine learning and DPI, this research offers a more robust method for detecting and preventing sophisticated cyber threats, thereby reducing the risk of successful data breaches and system sabotages in enterprise networks.

2. RESEARCH METHOD

In this study, the RapidMiner simulator is used for the APT Attack Data Exfiltration Phase detection and classification process. The methodological process is illustrated in Figure 1. According to Figure 1, the proposed methodology includes 4 modules, each of which will be described in detail in the following. This study's modules include data collection from an external source, preprocessing, classifiers, and performance evaluation.

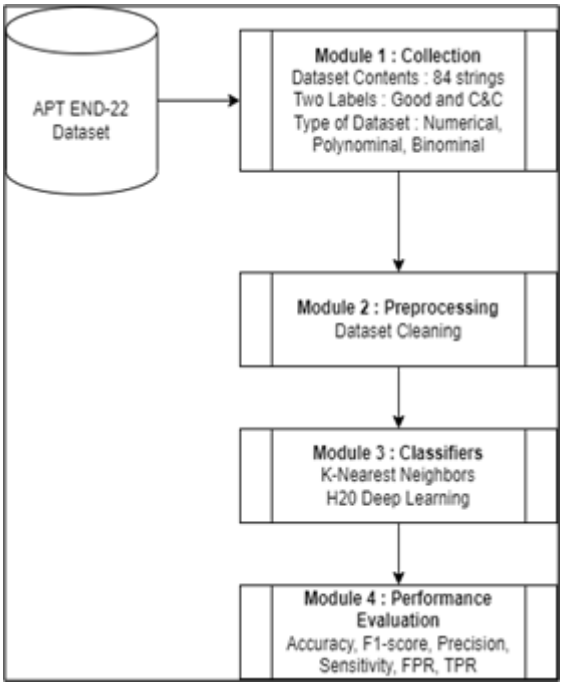


Figure 1. Proposed Method for Data Exfiltration Phase

2.1. END-22 Dataset

This work used the END-22 dataset to detect APT Data Exfiltration Phase. This dataset includes 84 network traffic data samples with packet anomaly and IP Address that labeled as Command & Control (C&C) that, known as APT Attacks signature. END-22 dataset features are described as shown in Table 1.

Table 1. Features of the END-22 Dataset

No.	Feature Name	Data Type
1	Alert Time	Numerical
2	Destination IP	Polynominal
3	Destination Reputation	Binominal
4	Inbound	Numerical
5	Outbound	Numerical
6	Sorce IP	Polynominal

2.2. Data Classifiers

This research compares the K-Nearest Neighbors and the H20 Deep Learning Model to measure the Performance of the Machine Learning methods used to analyze the Data Exfiltration Phase on the END-22 Dataset. H20 Deep Learning Model uses Deep Neural Networks [9], which uses multi-layered learning of the features as the main characteristic. These layers are called hidden layers in the neural network. A network is considered a deep learning network when it includes more than two hidden layers. It is necessary to mention that the advantage of a deep neural network is that it has lots of hidden layers, which makes it different from a superficial artificial neural network that has a single hidden layer. This means that deep neural networks can do more complex tasks. The structure of a deep network is such that the data is transferred from one hidden layer to another so that simpler features are recombined and recomposed as complex features [9].

The goal of deep learning is to discover several levels of distributed representations of the input data so that by creating features in the lower layers, it can differentiate the factors of changes in the input data and then combine these representations in the higher layers [13]. After entering the data into the deep network, the extraction of features and classification of the data exfiltration phase is performed simultaneously. No other method is required to extract the features because feature extraction is performed automatically

in a deep network. Finally, the data exfiltration classification is accomplished after applying the nonlinear function.

2.3. Performance Evaluation

This paper uses the confusion matrix in order to evaluate the machine learning models that we want to compare [14]. This matrix includes four elements, including True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) (See Table 2). TP represents that when an alert is generated, then an APT Data Exfiltration occurs. FP represents that when an alert is generated, but an APT Data Exfiltration does not occur. TN represents that when an alarm is not generated, then an APT Data Exfiltration does not occur. FN represents that when an alert is not generated, but an APT Data Exfiltration occurs.

Table 2. Confusion Matrix for Detection of APT Data Exfiltration

Actual Class	**Predicted Class**	
	Positive	**Negative**
Positive	True Positive (TP)	False Positive (FP)
Negative	False Negative (FN)	True Negative (TN)

According to the confusion matrix, we have used six criteria to evaluate two models, including the K-Nearest Neighbors and the H20 Deep Learning Model. The criteria are accuracy, F-measure or F1-score, precision or positive predictive value (PPV), specificity (TNR), sensitivity or true positive rate (TPR), and FPR [15]. These criteria are formulated based on the Equations 1-8 [7]. Furthermore, FPR and FNR criteria show the false, and FPR is a more important criterion than FNR regarding false determination and effectiveness. These criteria are formulated as follows. The results of the classification models will be analyzed in the next section.

$$TNR = \frac{TN}{TN + FP} \tag{1}$$

$$TPR = \frac{TP}{TP + FN} \tag{2}$$

$$Accuracy \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$Precison = \frac{Tp}{Tp + Fp} \tag{4}$$

$$Recall = \frac{Tp}{Tp + FN} \tag{5}$$

$$F - measure = 2 * \frac{precision * recall}{precision + recall} \tag{6}$$

$$FPR = 1 - TNR \tag{7}$$

$$FNR = 1 - TPR \tag{8}$$

3. RESULT AND ANALYSIS

The results of the K-Nearest Neighbours and H20 Deep Learning classification models are analyzed in this Section. Since this article aims to detect and classify APT Data Exfiltration on enterprise networks, we have used the END-22 dataset to detect the APT Data Exfiltration phase. After receiving the data and pre-processing, we used classification models such as K-Nearest Neighbours and H20 Deep Learning Model in the detection process. In addition, to evaluate the models in the output, criteria such as accuracy, precision, false positive rate (FPR), false negative rate (FNR), and F-measure were extracted as experiment results.The results based on the evaluation criteria are given in Table 3 for the K-Nearest Neighbours and H20 Deep Learning Model. According to Table 3,

the K-Nearest Neighbours and H20 Deep Learning Model accuracies are 71,43% and 90,48%, respectively. The FPR values, which is another important criterion, are 17,65% and 3,92% for the K-Nearest Neighbours and H20 Deep Learning Model. Furthermore, the rest of the evaluation criteria show that the proposed H20 Deep Learning Model has achieved the best results. Besides the criteria mentioned above, regarding TPR, TNR, F-Measure, and FNR values, the H20 Deep Learning Model performs better than the K-Nearest Neighbors Model. This research finds that the H20 Deep Learning model has the best performance in all the criteria to detect the APT Data Exfiltration phase on the END-22 dataset. While the results of the confusion matrix of each method are presented in Table 4 for K-Nearest Neighbors and Table 5 for H20 Deep Learning.

Table 3. Result of the Classification Models (%)

Classification Models	ACC	TPR	TNR	PPV	F-Measure	FPR	FNR
KNN	71.43	54.55	82.35	66.67	60	17.65	45.45
H20 Deep Learning Model	90.48	81.82	96.08	93.1	87	3.92	18.18

Table 4. Result of the Classification Models for K-Nearest Neighbours

Prediction	Actual	
	C&C	Good
C&C	18	9
Good	15	42

Table 5. Result of the Classification Models for H20 Deep Learning Model

Prediction	Actual	
	C&C	Good
Y6FGC&C	27	2
Good	6	49

In general, research indicates that machine learning methods are the best among approaches developed for APT attack detection. Moreover, according to the latest research in the field of network security, the deep learning method has the best performance compared to other methods. Consequently, this paper used machine learning methods such as K-Nearest Neighbours and H20 Deep Learning classification models to detect two normal and anomaly classes of the APT Data Exfiltration phase on the END-22 dataset. The models were implemented via RapidMiner software. As an APT attack is one of the most stable and persistent attacks on the system and involves the system for a long time, it is very important to detect it early. Therefore, artificial intelligence methods are essential for the timely detection of APT attacks, especially during the Data Exfiltration phase, where critical and sensitive data can be stolen from the victim, are essential.

4. CONCLUSION

In this study, two machine learning-based classification models including K-Nearest Neighbors and H20 Deep Learning were used to detect and classify APT attacks on the END-22 dataset. Since the nature of the APT attack is a permanent and persistent presence in the victims system, early detection of this attack requires high accuracy and minimal FPR in the early steps. For this purpose, through the mentioned classification models, based on the obtained results, a H20 deep learning model with the highest accuracy and the lowest FPR, which are equal to 90.48 and 3.92, respectively, was selected as the final model. In addition, other evaluation criteria, such as TPR, TNR, PPV, F-measure, FPR, and FNR were investigated. The H20 deep learning model also has the best performance in terms of these criteria.

The results indicate that deep learning is a highly effective approach for network security detection, particularly in identifying APT-related anomalies. The H2O Deep Learning model's superior performance suggests that it is well-suited for the early detection of APT attacks, thereby answering the research objective of identifying an effective method for detecting data exfiltration by APT threat actors. The findings of this study have significant implications for cybersecurity practices in enterprise environments. By demonstrating the effectiveness of combining machine learning techniques with Deep Packet Inspection (DPI), the research provides a valuable approach for enhancing the detection of data exfiltration attempts by Advanced Persistent Threat (APT) actors. This

improved detection capability can lead to the development of more advanced anomaly detection systems that can better protect enterprises from the covert and sophisticated attacks typically executed by APT groups. As a result, the study contributes to strengthening the overall cybersecurity posture of organizations, potentially reducing the risk of successful data breaches and system sabotage by state-sponsored cyber attackers. Additionally, the research emphasizes the importance of integrating advanced analytical methods into cybersecurity frameworks, which could influence future policies and strategies in enterprise-level cybersecurity. As for the future study, exploring a hybrid approach could be a good direction, that combines machine learning and deep learning methods to further enhance detection accuracy and reduce false positives. Additionally, the use of both supervised and unsupervised deep learning methods could be investigated on the END-22 dataset and other network traffic flows to identify new attack patterns and improve detection capabilities across different stages of APT attacks.

5. DECLARATIONS

AUTHOR CONTIBUTION

All authors contributed to this research

FUNDING STATEMENT

-

COMPETING INTEREST

The authors declare no competing interests regarding the data presented in this research.

REFERENCES

[1] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019, https://doi.org/10.1109/COMST.2019.2891891. [Online]. Available: https://ieeexplore.ieee.org/document/8606252

[2] D. Rahmawati, "BSSN Temukan 1,6 Miliar Serangan Siber Sepanjang 2021, Mayoritas Malware." [Online]. Available: https://news.detik.com/berita/d-5972491/bssn-temukan-1-6-miliar-serangan-siber-sepanjang-2021-mayoritas-malware

[3] S. Myneni, A. Chowdhary, A. Sabur, S. Sengupta, G. Agrawal, D. Huang, and M. Kang, "DAPT 2020 - Constructing a Benchmark Dataset for Advanced Persistent Threats: 1st International Workshop on Deployable Machine Learning for Security Defense, MLHat 2020, collocated with the 25th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD 2020," *Deployable Machine Learning for Security Defense - 1st International Workshop, MLHat 2020, Proceedings*, pp. 138–163, 2020, https://doi.org/10.1007/978-3-030-59621-7_8. [Online]. Available: http://www.scopus.com/inward/record.url?scp=85096612402&partnerID=8YFLogxK

[4] J. Chen, C. Su, K.-H. Yeh, and M. Yung, "Special Issue on Advanced Persistent Threat," *Future Generation Computer Systems*, vol. 79, pp. 243–246, Feb. 2018, https://doi.org/10.1016/j.future.2017.11.005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17324913

[5] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, and F. J. Aparicio-Navarro, "Detection of advanced persistent threat using machine-learning correlation analysis," *Future Generation Computer Systems*, vol. 89, pp. 349–359, Dec. 2018, https://doi.org/10.1016/j.future.2018.06.055. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18307532

[6] W.-L. Chu, C.-J. Lin, and K.-N. Chang, "Detection and Classification of Advanced Persistent Threats and Attacks Using the Support Vector Machine," *Applied Sciences*, vol. 9, no. 21, p. 4579, Jan. 2019, https://doi.org/10.3390/app9214579. [Online]. Available: https://www.mdpi.com/2076-3417/9/21/4579

[7] I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh, and D. M. Diab, "Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats," *IEEE Access*, vol. 7, pp. 99 508–99 520, 2019, https://doi.org/10.1109/ACCESS.2019.2930200. [Online]. Available: https://ieeexplore.ieee.org/document/8767917

[8] B. Mukherjee, L. Heberlein, and K. Levitt, "Network intrusion detection," *IEEE Network*, vol. 8, no. 3, pp. 26–41, May 1994, https://doi.org/10.1109/65.283931. [Online]. Available: https://ieeexplore.ieee.org/document/283931

[9] J. Hassannataj Joloudari, M. Haderbadi, A. Mashmool, M. Ghasemigol, S. S. Band, and A. Mosavi, "Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning," *IEEE Access*, vol. 8, pp. 186 125–186 137, 2020, https://doi.org/10.1109/ACCESS.2020.3029202. [Online]. Available: https://ieeexplore.ieee.org/document/9214817/

[10] A. Dijk, "Detection of Advanced Persistent Threats using Artificial Intelligence for Deep Packet Inspection," in *2021 IEEE International Conference on Big Data (Big Data)*, Dec. 2021, pp. 2092–2097, https://doi.org/10.1109/BigData52589.2021.9671464. [Online]. Available: https://ieeexplore.ieee.org/document/9671464

[11] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and V.-L. Nguyen, "An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection," *IEEE Access*, vol. 8, pp. 30 387–30 399, 2020, https://doi.org/10.1109/ACCESS.2020.2973023. [Online]. Available: https://ieeexplore.ieee.org/document/8990084

[12] J. V. BibalBenifa, S. Krishnann, H. Long, R. Kumar, and D. Taniar, "Performance Analysis of Machine Learning and Pattern Matching Techniques for Deep Packet Inspection in Firewalls," Sep. 2021, https://doi.org/10.21203/rs.3.rs-260788/v1. [Online]. Available: https://www.researchsquare.com/article/rs-260788/v1

[13] M. Lngkvist, L. Karlsson, and A. Loutfi, "A review of unsupervised feature learning and deep learning for time-series modeling," *Pattern Recognition Letters*, vol. 42, pp. 11–24, Jun. 2014, https://doi.org/10.1016/j.patrec.2014.01.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167865514000221

[14] S. Mojrian, G. Pinter, J. H. Joloudari, I. Felde, A. Szabo-Gali, L. Nadai, and A. Mosavi, "Hybrid Machine Learning Model of Extreme Learning Machine Radial basis function for Breast Cancer Detection and Diagnosis; a Multilayer Fuzzy Expert System," in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, Oct. 2020, pp. 1–7, https://doi.org/10.1109/RIVF48685.2020.9140744. [Online]. Available: https://ieeexplore.ieee.org/document/9140744

[15] J. H. Joloudari, H. Saadatfar, A. Dehzangi, and S. Shamshirband, "Computer-aided decision-making for predicting liver disease using PSO-based optimized SVM with feature selection," *Informatics in Medicine Unlocked*, vol. 17, p. 100255, Jan. 2019, https://doi.org/10.1016/j.imu.2019.100255. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352914819302539