Sakarya University Journal of Computer and Information Sciences
http://saucis.sakarya.edu.tr/

DOI: 10.35377/saucis...1379047 RESEARCH ARTICLE

A Systematic Review for Misuses Attack Detection based on Data Mining in NFV

Nebras Jalel Ibrahim [1], Ahmed K. Abbas [2], Farah Hatem Khorsheed [3]

[1] Computer Center, University of Diyala, Diyala / Iraq
[2] Collage of Education for pure science, University of Diyala, Diyala / Iraq
[3] Computer Center, University of Diyala, Diyala / Iraq

Corresponding author:
Ahmed K. Abbas, College of Education for Pure Science, Diyala University, Diyala-Iraq
E-mail address:
dr.ahmed.k.abbas@uodiyala.edu.iq

Submitted: 20 October 2023
Revision Requested: 11 December 2023
Last Revision Received: 19 December 2023
Accepted: 20 December 2023
Published Online: 27 December 2023

Citation: N. Ibrahim, A. Abbas, and F. Khorsheed, (2023). A Systematic Review for Misuses Attack Detection based on Data Mining I n NFV. *Sakarya University Journal of Computer and Information Sciences*, 6 (3) https://doi.org/10.35377/saucis...1379047

ABSTRACT

Network Function Virtualization could be a quickly advancing innovation that guarantees to revolutionize the way networks are planned, sent, and overseen. However, as with any modern innovation, there are potential security risk that must be tended to guarantee the security of the network. Misuses attacks are one such risk that can compromise the security and integrity of NFV frameworks.

In recently years , data mining has risen as a promising approach for recognizing misuses attacks in NFV systems. The novelty of this systematic mapping study is ponders points to supply an overview of the existing research on misuses attack detection based on data mining in NFV. Particularly, the study will recognize and analyze the research conducted in this region, counting the sorts of data mining methods utilized, the types of misuses attacks identified, and the assessment strategies utilized.

The results of this study will give experiences into the current state of investigate on misuses attack detection based on data mining in NFV, as well as recognize gaps and openings for future research in this range. Also, the study will serve as an important asset for analysts and professionals looking for to create successful and effective methods for recognizing misuses attacks in NFV frameworks

Keywords: Misuses attack detection, Data mining, Network Function Virtualization (NFV), Systematic mapping

1. Introduction

Network Function Virtualization (NFV) is a technology that enables the deployment of network functions as software-based services that can run on standard servers and cloud infrastructure. NFV promises to reduce costs, improve network flexibility, and accelerate service delivery. However, the use of NFV also introduces new security challenges that need to be addressed [1].

One of the primary security concerns in NFV systems is the threat of misuses attacks. Misuses attacks occur when an attacker misuses a legitimate access point or privilege to gain unauthorized access to the network or its resources [2]. These attacks can result in data breaches, service disruptions, and other serious security incidents. To address the threat of misuses attacks in NFV systems, researchers have explored the use of data mining techniques for detecting such attacks. Data mining is a process of discovering patterns and knowledge from large datasets using statistical and computational techniques [3].

The use of data mining for detecting misuses attacks in NFV systems has several advantages. It allows for the detection of previously unknown attacks, can identify complex attack patterns, and can be used to analyze large amounts of network data in real-time [4].

This systematic mapping study aims to provide an overview of the existing research on misuses attack detection based on data mining in NFV [5]. The study will identify the types of data mining techniques used, the types of misuses attacks detected, and the evaluation methods employed in previous research [6]. The results of this study will help researchers and practitioners to develop more effective and efficient techniques for detecting misuses attacks in NFV systems, thereby enhancing the security and resilience of these systems.

2. Literature Review

Misuses attacks are one of the most significant security threats in NFV systems. As NFV systems are designed to be flexible and scalable, they are vulnerable to a wide range of misuses attacks that can compromise their security and integrity. Therefore, researchers have been exploring various techniques to detect misuses attacks in NFV systems.

Shilan S. Hameed et al 2021 designed a systematic review that explores the role of machine learning approaches in addressing the security requirements of IoT devices and systems. The authors created a list of research questions, the authors searched for relevant papers from different databases including IEEE, Web of Science, Springer Link, Scopus, and Science Direct. The most specific and relevant papers were extracted to answer the research questions. Later on, the selected papers were comprehensively screened and analyzed. Finally, the results were presented using different methods [7].

In another study, Zhang et al. (2020) proposed a misuses attack detection system for NFV based on ensemble learning techniques. The proposed system combined multiple classifiers to improve the accuracy of misuses attack detection in NFV[8].

Additionally, Mohamed Amine Ferrag, Lei Shu, Hamouda Djallel, and Kim-Kwang Raymond Choo discuss the importance of implementing effective intrusion detection systems in the agriculture industry to prevent Distributed Denial of Service (DDoS) attacks[9].

In [10] Nadra Guizani and Arif Ghafoor from Purdue University (2020) discussed a network function virtualization system for detecting malware in large IoT based networks and addressed the challenges posed by the exponential growth of IoT devices and the need for effective software-based security systems.

Abdullah Emir Çil et al in 2021 proposed the use of a deep neural network (DNN) model to detect and classify DDoS attacks based on captured network traffic. The experiments conducted on a dataset of DDoS attacks showed a 99.99% success rate in detecting attacks and a 94.57% accuracy rate in classifying attack types. The study concludes that deep learning models, such as DNN, can be effectively used to combat DDoS attacks. Previous studies have also utilized deep learning models, such as Deep Belief Network (DBN), Stacked Autoencoders (SAE), Long Short-Term Memory (LSTM), and Deep Convolutional Neural Network (DCNN), for DDoS intrusion detection with high accuracy [30].

Overall, the literature suggests that data mining techniques have considerable potential for misuses attack detection in NFV systems. In [11] Sulaiman, N. S. et al. (2021) provide a comprehensive overview of various techniques used in detecting and preventing unauthorized access to computer systems. However, there is a need for further research to develop more effective and efficient techniques that can be applied to real-world NFV systems. The results of this systematic mapping study will help to identify gaps and opportunities for future research in this area.

3. Research Questions

The following are research questions that could guide a systematic mapping study for misuses attack detection based on data mining in NFV:

Q1\\ What are the databases that used in this study? And what are the models that are used to build different perspectives?

Q2\\ What Classification schemes have been used to assess the effectiveness of misuses attack detection based on data mining in NFV systems?

Q3\\ What types of misuses attacks have been detected using data mining techniques in NFV systems?

Q4\\ What are the types of data mining techniques that have been used for misuses attack detection in NFV systems?

3.1 Search Statement

The following is a search statement for a systematic mapping study on misuse attack detection based on data mining in Network Function Virtualization (NFV):

((((("misuse attack" OR "misuse detection") AND ("data mining" OR "machine learning" OR "deep learning" OR "artificial intelligence")) AND ("network function virtualization" OR "NFV")) AND ("systematic mapping" OR "systematic review" OR "systematic literature review" OR "mapping study"))

This search statement includes keywords related to misuse attack detection, data mining, machine learning, artificial intelligence, and NFV. The search statement also includes terms related to systematic mapping studies, which will help identify relevant research in this area.

3.2 Search in databases

There are many different databases and platforms used by publishers to manage their content and information. However, some of the most widely used publisher databases include:

1. **Scopus**: A bibliographic database of scientific literature, including journals, books, and conference proceedings, published by Elsevier [12]
2. **ACM digital library**: A digital library that provides access to thousands of academic journals, books, and primary sources in the humanities, social sciences, and sciences [13].
3. **ProQuest**: A provider of digital information and research tools, including databases of academic journals, newspapers, and dissertations [14].
4. **IEEE Xplore**: A digital library of scientific and technical content published by the Institute of Electrical and Electronics Engineers (IEEE) [15].
5. **Springer**: is an international publisher that offers a wide range of opportunities for authors, customers, and partners. Springer is a leading scientific publisher that publishes in various fields [16].

We collected the papers in this study depending on the databases above (Appendix A).

4. Screening of Papers

In a systematic mapping review, the screening process typically involves several stages to identify relevant papers that will be included in the review [17]. The following are the general steps involved in the screening process. The figure below explains these steps:

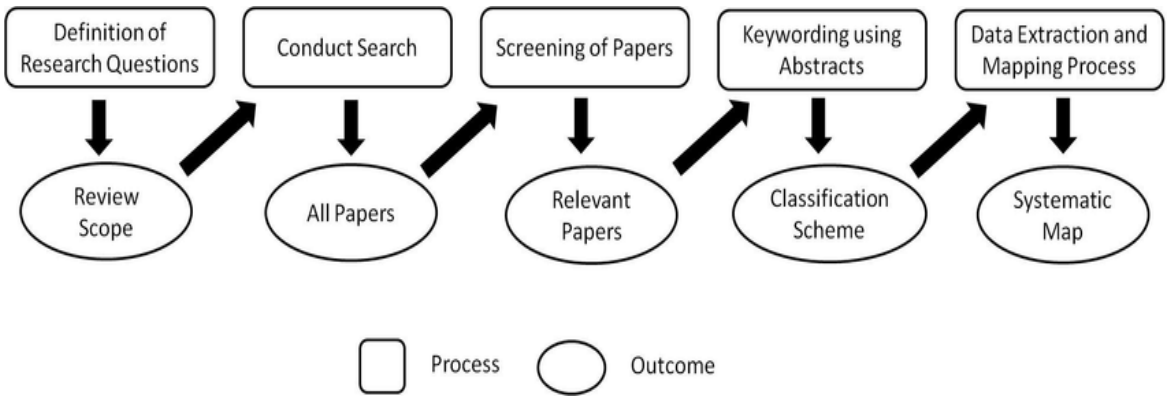

Figure 1. Systematic review process

4.1 Use various models to build different perspectives

We can explain any schema or description of any topic by constructing schemas. Define an overall vision for the article on each topic and approach it with some options. In this article, we show how to use these scenarios as we explain below.

A. Distribution of studies according to years

This graph shows the distribution of the number of studies per year and the percentage of publications per year, it focuses on which papers have full pages or short pages.

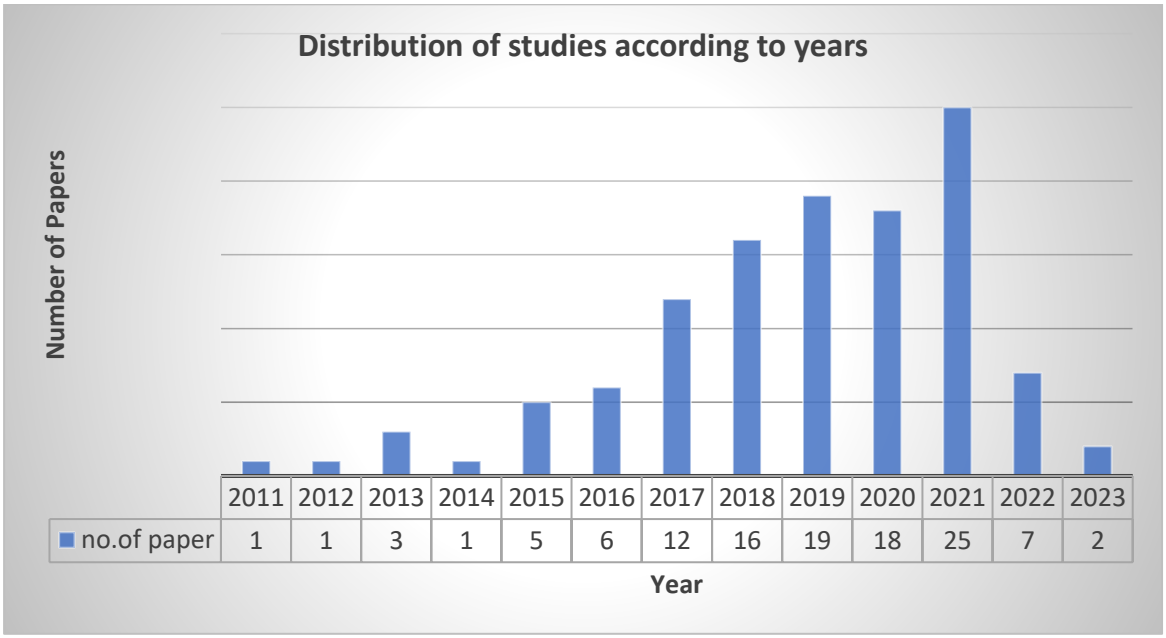

Figure 2. The distribution of studies in each year

B. Distribution of studies according to Publication type

The chart offers researchers a different perspective. Distribute papers by year, number of short or full-page papers, and paper type for conferences and journals.

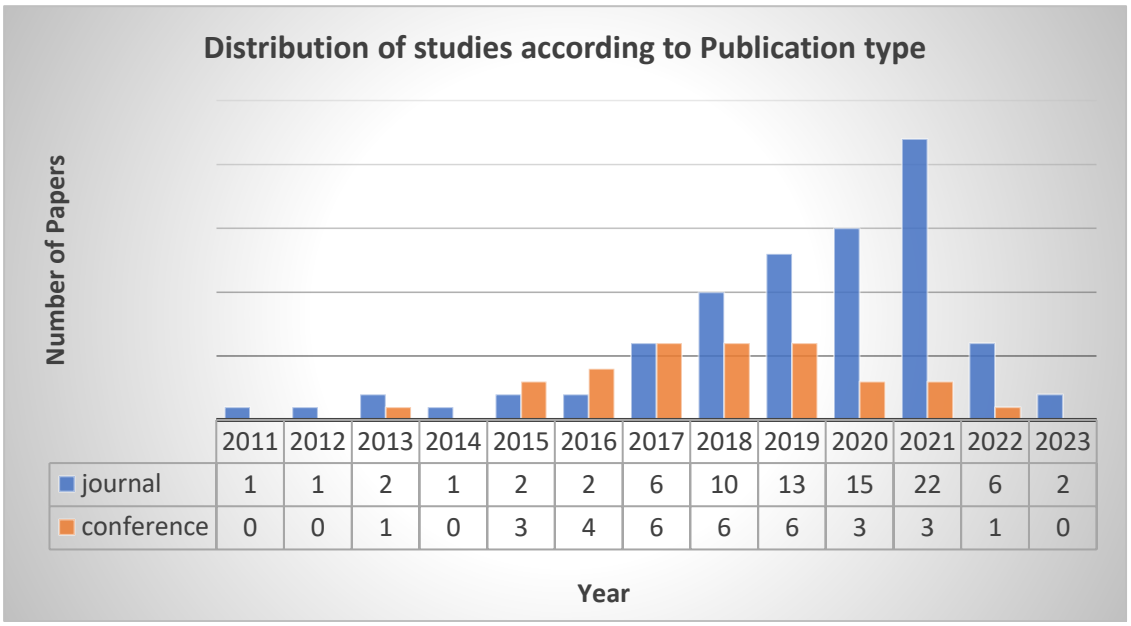

Figure 3. The Distribution of studies according to publication type

C. Distribution of studies according to Country

This chart shows the distribution of the number of studies per country.

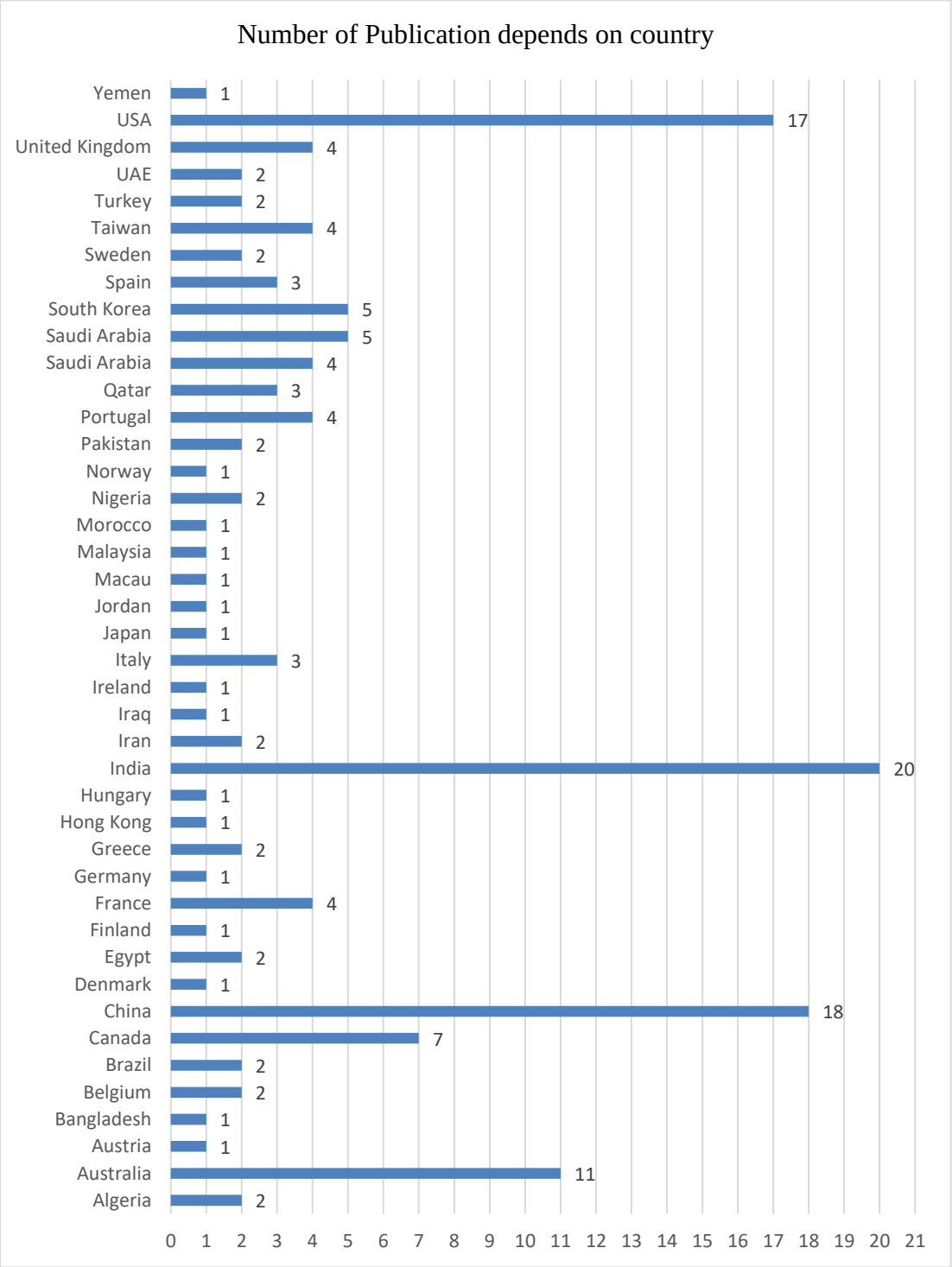

Figure 4. Distribution of studies according to country

5. Classification schemes

Systematic reviews are an important tool for synthesizing and summarizing the available evidence on a particular topic[18]. When it comes to classification schemes for systematic reviews of misuses attack detection based on data mining in NFV, there are a few different approaches that could be taken. Here are a few possibilities:

A. Type of attack:

One approach to classification could be to focus on the different types of attacks that are being detected using data mining techniques in NFV. This could include things like DDoS attacks, malware infections, phishing attempts, and so on.

Misuse attacks are a type of attack that involves exploiting vulnerabilities or weaknesses in a system by using legitimate functionality in an unauthorized or unintended way[19]. Misuse attacks can take many different forms, and the specific types of attacks that are relevant for misuses attack detection based on data mining in NFV may vary depending on the specific security domains and architectures being considered.

However, here are some common types of misuse attacks that could be relevant for misuses attack detection based on data mining in NFV:

1. **Denial-of-Service (DoS) attacks**: These attacks involve overwhelming a system or network with traffic or requests to make it unavailable to users. DoS attacks can be launched from multiple sources and can be difficult to detect and mitigate[20].
2. **Injection attacks**: These attacks involve injecting malicious code or data into a system or network, such as SQL injection or cross-site scripting (XSS) attacks. Injection attacks can bypass security measures and enable attackers to steal data or take control of systems[21].
3. **Malware attacks**: These attacks involve infecting systems or networks with malware, such as viruses, worms, or trojans. Malware can be used to steal data, disrupt operations, or launch further attacks[22].
4. **Brute-force attacks**: These attacks involve guessing passwords or other authentication credentials through trial and error. Brute-force attacks can be time-consuming but can be successful if passwords are weak or easily guessable[23].
5. **Evasion attacks**: These attacks involve attempting to bypass or evade security measures, such as by exploiting weaknesses in firewalls or intrusion detection systems. Evasion attacks can be difficult to detect and mitigate because they are designed to avoid detection[24].

The other attacks are:

- Unauthorized access. Unauthorized access refers to attackers accessing a network without receiving permission.
- Man in the middle attacks.
- Code and SQL injection attacks.
- Privilege escalation.
- Insider threats.

These are just a few examples of the types of misuse attacks that could be relevant for misuses attack detection based on data mining in NFV. The specific types of attacks will depend on the context and the security domains being considered.

B. Data mining techniques:

Another approach could be to classify the different data mining techniques that are being used to detect misuses attacks in NFV. For example, one review might focus on studies that use decision trees, while another might focus on those that use neural networks or support vector machines.

There are several data mining techniques that can be used for misuses attack detection based on data mining in NFV. Here are some examples:

1. **Decision Trees**: Decision trees are a popular data mining technique for classification tasks. In the context of misuse attack detection in NFV, decision trees can be used to classify network traffic as either normal or malicious based on various features or attributes, such as packet size, protocol, or source IP address[25].
2. **Neural Networks**: Neural networks are another popular data mining technique that can be used for classification and prediction tasks. In the context of misuse attack detection in NFV, neural networks can be trained on historical network traffic data to identify patterns and anomalies that are indicative of malicious activity[26].
3. **Support Vector Machines (SVMs)**: SVMs are a type of machine learning algorithm that can be used for classification and regression tasks. In the context of misuse attack detection in NFV, SVMs can be used to classify network traffic as either normal or malicious based on a set of features or attributes[27].
4. **Clustering**: Clustering is a data mining technique that involves grouping similar data points together based on their characteristics. In the context of misuse attack detection in NFV, clustering can be used to identify groups of network traffic that exhibit similar patterns or behaviors, which can then be analyzed further for potential malicious activity[28].
5. **Association Rule Mining**: Association rule mining is a data mining technique that involves identifying relationships or associations between different variables or attributes in a dataset. In the context of misuse attack detection in NFV,

association rule mining can be used to identify patterns or relationships between different network traffic features or attributes that are indicative of malicious activity[29].

Table 1. The intersection between types of misuse attack with data mining techniques.

Types of misuse attack	Denial of Services (DoS) attacks	Injection attacks	Malware attacks	Brute-force attacks	Evasion attacks	Others
Decision Tree	1,2,3,5,6,7,15,17,19,20, 21,12,23,2,26,33,35,47, 50,51,52,53,56,57,59,60 ,62,63,65,69,70,71,73,7 5,78,81,85,87,88,89,90, 94,99,100,101,102,103, 107,111,112,113,114,11 5, 116	17,25,26,52 ,57,70,71,8 5,99	17,19,21,23, 30,31,47,50, 52,60,62,63, 65,69,75,85, 89,90,99,10 5,114	1	3,75	10,6,29,123 ,148
Neural Networks	1,6,8,14,15,19,20,21,13, 14,17,23,25,26,33,34,35 ,36,41,42,46,47,49,50,5 1,52,53,55,56,57,58,59, 60,62,63,65,67,69,71,73 ,74,75,76,78,79,81,83,8 5,87,88,89,90,92,94,96, 99,100,101,102,103,107 ,110,111,112,113,114,1 15,116	14,25,26,32 ,42,46,48,4 9,52,57,71, 85,99	8,13,14,19,1 7,21,23,30,3 1,35,41,42,4 3,46,47,50,5 2,56,60,62,6 3,65,69,75,7 9,83,85,89,9 0,92,96,99,1 05,110,114	1,56	75,83	,29,10,61,8 2,116
Support Vector Machine (SVM)	1,2,6,14,15,17,20,21,12, 23,26,29,33,34,35,45,46 ,47,49,50,51,52,53,54,5 5,56,57,58,59,62,62,63, 67,70,71,73,74,77,78,79 ,85,87,88,89,90,91,92,9 4,99,101,102,103,104,1 07,111,112,114,115,116	14,26,32,46 ,48,49,52,5 7,70,71,77, 85,99	12,14,18,21, 23,29,30,35, 46,47,50,52, 56,60,62,63, 77,79,85,89, 90,92,99,11 4	1,56		,10,6
Clustering	1,6,8,7,19,20,21,11,13,2 3,29,33,35,37,41,50,51, 52,55,58,59,60,62,63,65 ,70,71,73,76,77,78,85,8 8,89,90,91,99,100,101,1 04,110,114,115,116	37,32,52,70 ,71,77,85,9 9	12,19,13,21, 23,29,30,31, 35,37,50,52, 60,62,63,65, 77,79,85,89, 90,99,110,1 14	1		6,5,10,12,2 9,116
Association Rule Mining	20,33,59,63,71,79,90, 104	71	30,63,79			10,12

Table 1 above represents the intersection between Data mining techniques and types of misuse attacks and Figure 5 below represents facet 1 (Types of misuse attacks with data mining techniques).

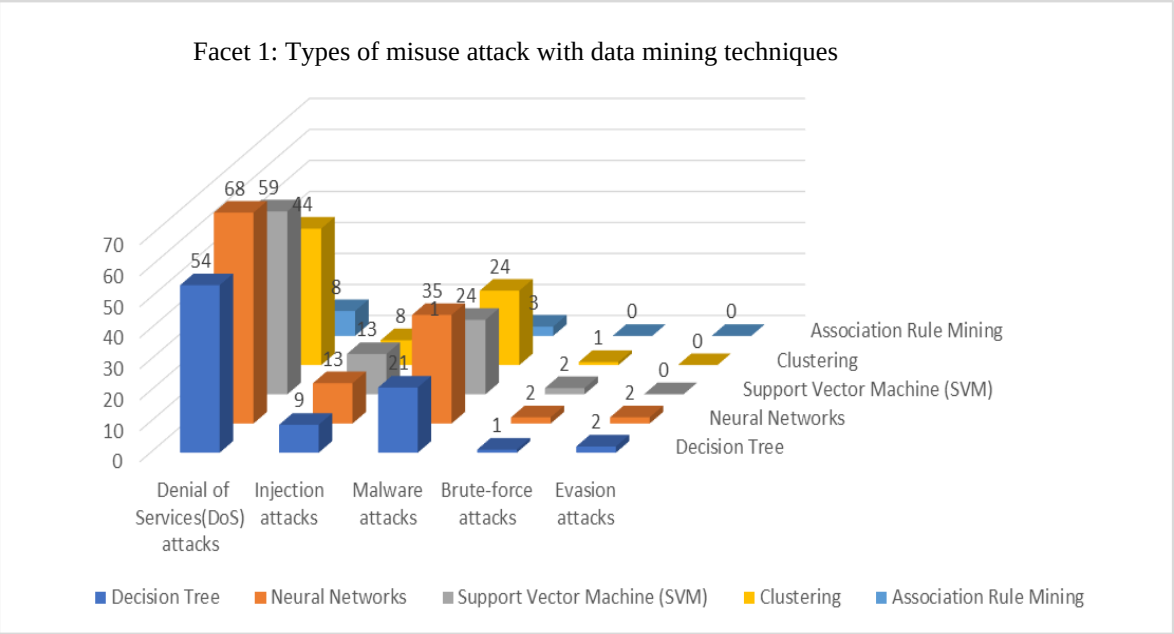

Figure 5. Types of misuse attack with data mining techniques

6. Conclusion and Comments

In conclusion, this systematic mapping study focused on the detection of misuses attacks in Network Function Virtualization (NFV) using data mining techniques. Through a comprehensive analysis of the existing literature, we identified and synthesized relevant studies, highlighting the various approaches, methodologies, and tools employed in this domain. The findings reveal that data mining plays a crucial role in the detection of misuses attacks in NFV, enabling the identification of anomalous patterns and the timely mitigation of potential threats. In this study, we apply different approaches like Type of attack and Data mining techniques as a classification schema and we note that most studies were used the Denial of Services (DoS) attacks with Decision Tree, Neural Networks, Support Vector Machine (SVM) and Clustering and at a lower frequency between Malware attacks and Decision Tree, Neural Networks, Support Vector Machine (SVM) and Clustering While attacks of Injection attacksو Brute-force attacks and Evasion attacks with data mining techniques this types have been studied very little compared to other types. The study also emphasizes the need for further research to address existing gaps, such as the development of more robust and efficient algorithms, the consideration of real-time detection, and the exploration of novel data sources. Ultimately, this systematic mapping study provides a valuable foundation for future researchers, practitioners, and stakeholders, serving as a reference point for advancing the field of misuses attack detection in NFV through data mining methodologies.

References

[1] Firoozjaei, M. D., Jeong, J. P., Ko, H., & Kim, H. (2017). Security challenges with network functions virtualization. Future Generation Computer Systems, 67, 315-324.
[2] Alnaim, A. K., Alwakeel, A. M., & Fernandez, E. B. (2022). Towards a security reference architecture for NFV. Sensors, 22(10), 3750.
[3] Guleria, P., & Sood, M. (2014). Data mining in education: A review on the knowledge discovery perspective. International Journal of Data Mining & Knowledge Management Process, 4(5), 47.
[4] Saeed, M. M. (2022). A real-time adaptive network intrusion detection for streaming data: a hybrid approach. Neural Computing and Applications, 34(8), 6227-6240.
[5] Abbas, A. K., Fleh, S. Q., & Safi, H. H. (2015). Systematic Mapping Study On Managing Variability In Software Product Line Engineering: Communication. Diyala Journal of Engineering Sciences, 511-520.
[6] Fleh, S. Q., Abbas, A. K., & Saffer, K. M. (2015, December). A systematic mapping study on runtime monitoring of services. In The Iraqi Journal For Mechanical And Material Engineering, Special for Babylon First International Engineering Conference, Issue (A).
[7] Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. PeerJ Computer Science, 7, e414.
[8] Zhao, Y., Li, Y., Zhang, X., Geng, G., Zhang, W., & Sun, Y. (2019). A survey of networking applications applying the software defined networking concept based on machine learning. IEEE Access, 7, 95397-95417.
[9] Ferrag, M. A., Shu, L., Djallel, H., & Choo, K. K. R. (2021). Deep learning-based intrusion detection for distributed

denial of service attack in agriculture 4.0. Electronics, 10(11), 1257.
[10] Guizani, N., & Ghafoor, A. (2020). A network function virtualization system for detecting malware in large IoT based networks. IEEE Journal on Selected Areas in Communications, 38(6), 1218-1228.
[11] Sulaiman, N. S., Nasir, A., Othman, W. R. W., Wahab, S. F. A., Aziz, N. S., Yacob, A., & Samsudin, N. (2021, May). Intrusion detection system techniques: a review. In Journal of Physics: Conference Series (Vol. 1874, No. 1, p. 012042). IOP Publishing.
[12] Elsevier, https://www.elsevier.com
[13] Association for Computing Machinery, https://dl.acm.org/.
[14] Proquest, https://www.proquest.com/.
[15] IEEE, https://ieeexplore.ieee.org/Xplore/home.jsp.
[16] Springer, https://www.springer.com/gp.
[17] Lopez-Herrejon, R. E., Linsbauer, L., & Egyed, A. (2015). A systematic mapping study of search-based software engineering for software product lines. Information and software technology, 61, 33-51.
[18] Aromataris, E., Fernandez, R., Godfrey, C. M., Holly, C., Khalil, H., & Tungpunkom, P. (2015). Summarizing systematic reviews: methodological development, conduct and reporting of an umbrella review approach. JBI Evidence Implementation, 13(3), 132-140.
[19] Shanmugam, B., & Idris, N. B. (2009, December). Improved intrusion detection system using fuzzy logic for detecting anomaly and misuse type of attacks. In 2009 International Conference of Soft Computing and Pattern Recognition (pp. 212-217). IEEE.
[20] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials, 18(1), 602-622.
[21] Sharma, P., Johari, R., & Sarma, S. S. (2012). Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. International Journal of System Assurance Engineering and Management, 3, 343-351.
[22] Kaur, J. (2019). Taxonomy of malware: virus, worms and trojan. Int. J. Res. Anal. Rev, 6(1), 192-196.
[23] Khan, H. Z. U., & Zahid, H. (2010). Comparative study of authentication techniques. International Journal of Video & Image Processing and Network Security IJVIPNS, 10(04), 09-13.
[24] Corona, I., Giacinto, G., & Roli, F. (2013). Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. Information Sciences, 239, 201-225.
[25] Sharma, H., & Kumar, S. (2016). A survey on decision tree algorithms of classification in data mining. International Journal of Science and Research (IJSR), 5(4), 2094-2097.
[26] Stahl, F., & Jordanov, I. (2012). An overview of the use of neural networks for data mining tasks. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2(3), 193-208.
[27] Marir, N., Wang, H., Feng, G., Li, B., & Jia, M. (2018). Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using spark. IEEE Access, 6, 59657-59671.
[28] Berkhin, P. (2006). A survey of clustering data mining techniques. In Grouping multidimensional data: Recent advances in clustering (pp. 25-71). Berlin, Heidelberg: Springer Berlin Heidelberg.
[29] Treinen, J. J., & Thurimella, R. (2006). A framework for the application of association rule mining in large intrusion detection infrastructures. In Recent Advances in Intrusion Detection: 9th International Symposium, RAID 2006 Hamburg, Germany, September 20-22, 2006 Proceedings 9 (pp. 1-18). Springer Berlin Heidelberg.
[30] Cil, A. E., Yildiz, K., & Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems with Applications*, *169*, 114520.

Appendix A

1. Gulzar, B., & Gupta, A. (2021). DAM: a theoretical framework for SensorSecurity in IoT applications. International Journal of Next-Generation Computing, 12(3), 10-47164.
2. Zhao, S., Chandrashekar, M., Lee, Y., & Medhi, D. (2015, March). Real-time network anomaly detection system using machine learning. In 2015 11th international conference on the design of reliable communication networks (drcn) (pp. 267-270). IEEE.
3. Barradas, D., Santos, N., Rodrigues, L., Signorello, S., Ramos, F. M., & Madeira, A. (2021, February). FlowLens: Enabling Efficient Flow Classification for ML-based Network Security Applications. In NDSS.
4. Baktayan, A., & Albaltah, I. A. (2022). A blockchain-based trust management system for 5G network slicing enabled C-RAN. Sustainable Engineering and Innovation, 4(1), 8.
5. Lee, S., Kim, J., Shin, S., Porras, P., & Yegneswaran, V. (2017, June). Athena: A framework for scalable anomaly detection in software-defined networks. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 249-260). IEEE.
6. Li, J., Zhao, Z., & Li, R. (2017). A machine learning based intrusion detection system for software defined 5G network. *arXiv preprint arXiv:1708.04571*.
7. Li, J., Zhao, Z., Li, R., & Zhang, H. (2018). Ai-based two-stage intrusion detection for software defined iot

networks. *IEEE Internet of Things Journal*, *6*(2), 2093-2102.
8. Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, *8*(4), 2300-2317.
9. Jauro, F., Chiroma, H., Gital, A. Y., Almutairi, M., Shafi'i, M. A., & Abawajy, J. H. (2020). Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend. *Applied Soft Computing*, *96*, 106582.
10. Zou, D., Lu, Y., Yuan, B., Chen, H., & Jin, H. (2018). A fine-grained multi-tenant permission management framework for SDN and NFV. *IEEE Access*, *6*, 25562-25572.
11. Darwish, T. S., & Bakar, K. A. (2018). Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues. *IEEE Access*, *6*, 15679-15701.
12. Corrêa, J. H., Ciarelli, P. M., Ribeiro, M. R., & Villaça, R. S. (2021). Ml-based ddos detection and identification using native cloud telemetry macroscopic monitoring. *Journal of Network and Systems Management*, *29*, 1-28.
13. Alharbi, T., Aljuhani, A., & Taylor, B. (2019). A collaborative SYN flooding detection ApproachA collaborative SYN. *International Journal of Computer Engineering and Information Technology*, *11*(9), 186-196.
14. Zhou, C., Hu, B., Shi, Y., Tian, Y. C., Li, X., & Zhao, Y. (2020). A unified architectural approach for cyberattack-resilient industrial control systems. *Proceedings of the IEEE*, *109*(4), 517-541.
15. Ferrag, M. A., Shu, L., Djallel, H., & Choo, K. K. R. (2021). Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics*, *10*(11), 1257.
16. Zhang, H., Wang, Y., Chen, H., Zhao, Y., & Zhang, J. (2017). Exploring machine-learning-based control plane intrusion detection techniques in software defined optical networks. *Optical Fiber Technology*, *39*, 37-42.
17. Salahdine, F., Han, T., & Zhang, N. (2023). Security in 5G and beyond recent advances and future challenges. *Security and Privacy*, *6*(1), e271.
18. DEORE, M., MANE, D., UPADHYE, G., & KITTAD, N. (2022). THE SECURITY CONCERNS AND SOLUTIONS FOR CLOUD-BASED IOT SYSTEM. *Journal of Theoretical and Applied Information Technology*, *100*(18).
19. Kim, H., Kim, J., Kim, Y., Kim, I., & Kim, K. J. (2019). Design of network threat detection and classification based on machine learning on cloud computing. *Cluster Computing*, *22*, 2341-2350.
20. D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2020). Inter-dataset generalization strength of supervised machine learning methods for intrusion detection. *Journal of Information Security and Applications*, *54*, 102564.
21. Ahmad, I., Shahabuddin, S., Malik, H., Harjula, E., Leppänen, T., Loven, L., ... & Riekki, J. (2020). Machine learning meets communication networks: Current trends and future challenges. *IEEE Access*, *8*, 223418-223460.
22. Kulkarni, P., & Cauvery, N. K. (2021). Personally Identifiable Information (PII) Detection in the Unstructured Large Text Corpus using Natural Language Processing and Unsupervised Learning Technique. *International Journal of Advanced Computer Science and Applications*, *12*(9).
23. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *Ieee access*, *6*, 35365-35381.
24. Yang, H. (2020, October). Research on Classification Algorithm for Civil Aviation Internal Network Intrusion Detection Based on Machine Learning. In *2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT* (pp. 1-4). IEEE.
25. Riera, T. S., Higuera, J. R. B., Higuera, J. B., Herraiz, J. J. M., & Montalvo, J. A. S. (2022). A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques. *Computers & Security*, *120*, 102788.
26. Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M. A., Mukherjee, M., & Khan, F. A. (2019). Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors*, *19*(14), 3119.
27. Adhikari, N., & Ramkumar, M. (2023). IoT and Blockchain Integration: Applications, Opportunities, and Challenges. *Network*, *3*(1), 115-141.
28. Overmars, A., & Venkatraman, S. (2020). Towards a secure and scalable iot infrastructure: A pilot deployment for a smart water monitoring system. *Technologies*, *8*(4), 50.
29. Al Makdi, K., Sheldon, F. T., & Hussein, A. A. (2020, November). Trusted Security Model for IDS Using Deep Learning. In *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)* (pp. 1-4). IEEE.
30. Liu, Y., Yu, F. R., Li, X., Ji, H., & Leung, V. C. (2020). Blockchain and machine learning for communications and networking systems. *IEEE Communications Surveys & Tutorials*, *22*(2), 1392-1431.
31. Zago, M., Gil Pérez, M., & Martínez Pérez, G. (2021). Early DGA-based botnet identification: pushing detection to the edges. *Cluster Computing*, 1-16.
32. Bertero, C., Roy, M., Sauvanaud, C., & Trédan, G. (2017, October). Experience report: Log mining using natural language processing and application to anomaly detection. In *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)* (pp. 351-360). IEEE.
33. D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2019). In-depth comparative evaluation of supervised machine learning approaches for detection of cybersecurity threats. In *4th International Conference on Internet of Things, Big Data and Security (IoTBDS)* (pp. 125-136).
34. Phan, T. V., & Park, M. (2019). Efficient distributed denial-of-service attack defense in SDN-based cloud. *IEEE Access*, *7*, 18701-18714.
35. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2017). HAST-IDS: Learning hierarchical

spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE access*, *6*, 1792-1806.
36. Soldani, D. (2020). On Australia's cyber and critical technology international engagement strategy towards 6G: How Australia May become a leader in cyberspace. *Journal of Telecommunications and the Digital Economy*, *8*(4), 127-158.
37. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, *7*(10), 10250-10276.
38. Padhi, P. K., & Charrua-Santos, F. (2021). 6G enabled tactile internet and cognitive internet of healthcare everything: Towards a theoretical framework. *Applied System Innovation*, *4*(3), 66.
39. Aazam, M., Zeadally, S., & Harras, K. A. (2018). Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Transactions on Industrial Informatics*, *14*(10), 4674-4682.
40. Zunino, C., Valenzano, A., Obermaisser, R., & Petersen, S. (2020). Factory communications at the dawn of the fourth industrial revolution. *Computer Standards & Interfaces*, *71*, 103433.
41. Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., ... & Toka, L. (2020). 5g support for industrial iot applications—challenges, solutions, and research gaps. *Sensors*, *20*(3), 828.
42. Ferrag, M. A., & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet of Things Journal*, *8*(24), 17236-17260.
43. Joshi, K. D., & Kataoka, K. (2020). pSMART: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN. *Computer Networks*, *178*, 107295.
44. Gedeon, J., Brandherm, F., Egert, R., Grube, T., & Mühlhäuser, M. (2019). What the fog? edge computing revisited: Promises, applications and future challenges. *IEEE Access*, *7*, 152847-152878.
45. Wang, Y., Meng, W., Li, W., Liu, Z., Liu, Y., & Xue, H. (2019). Adaptive machine learning-based alarm reduction via edge computing for distributed intrusion detection systems. *Concurrency and Computation: Practice and Experience*, *31*(19), e5101.
46. Tien, C. W., Huang, T. Y., Tien, C. W., Huang, T. C., & Kuo, S. Y. (2019). Kubanomaly: anomaly detection for the docker orchestration platform with neural network approaches. *Engineering reports*, *1*(5), e12080.
47. Abbasi, H., Ezzati-Jivan, N., Bellaiche, M., Talhi, C., & Dagenais, M. R. (2019). Machine learning-based EDoS attack detection technique using execution trace analysis. *Journal of Hardware and Systems Security*, *3*, 164-176.
48. Tekerek, A. (2021). A novel architecture for web-based attack detection using convolutional neural network. *Computers & Security*, *100*, 102096.
49. Ujjan, R. M. A., Pervez, Z., Dahal, K., Bashir, A. K., Mumtaz, R., & González, J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. *Future Generation Computer Systems*, *111*, 763-779.
50. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, *7*, 100059.
51. Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications*, *53*, 102532.
52. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *Ieee Access*, *7*, 41525-41550.
53. Wang, M., Zheng, K., Yang, Y., & Wang, X. (2020). An explainable machine learning framework for intrusion detection systems. *IEEE Access*, *8*, 73127-73141.
54. Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2018, December). Detection of DDoS attack on SDN control plane using hybrid machine learning techniques. In *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 299-303). IEEE.
55. Yang, K., Ren, J., Zhu, Y., & Zhang, W. (2018). Active learning for wireless IoT intrusion detection. *IEEE Wireless Communications*, *25*(6), 19-25.
56. Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2020). Multi-stage optimized machine learning framework for network intrusion detection. IEEE Transactions on Network and Service Management, 18(2), 1803-1816.
57. Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2019, March). Design of ensemble learning methods for DDoS detection in SDN environment. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)* (pp. 1-6). IEEE.
58. Zhu, Y., Gaba, G. S., Almansour, F. M., Alroobaea, R., & Masud, M. (2021). Application of data mining technology in detecting network intrusion and security maintenance. Journal of Intelligent Systems, 30(1), 664-676.
59. Wu, K., & De Soto, B. G. (2022). Current State and Future Opportunities of Data Mining for Construction 4.0. In ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction (Vol. 39, pp. 78-85). IAARC Publications.
60. Sangwan, U., & Chhillar, R. S. (2022). Comparison of Various Classification Techniques in Cyber Security Using Iot. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(3), 334-339.
61. Nadig, D., Ramamurthy, B., Bockelman, B., & Swanson, D. (2018, March). Identifying anomalies in gridftp transfers for data-intensive science through application-awareness. In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 7-12).
62. Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. *Wireless communications and mobile computing*, *2021*,

1-17.
63. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. *IEEE communications surveys & tutorials*, *21*(1), 686-728.
64. Yousefian, N., Hansen, J. H., & Loizou, P. C. (2014). A hybrid coherence model for noise reduction in reverberant environments. *IEEE Signal Processing Letters*, *22*(3), 279-282.
65. Al-Hawawreh, M. S. (2017, May). SYN flood attack detection in cloud environment based on TCP/IP header statistical features. In *2017 8th International Conference on Information Technology (ICIT)* (pp. 236-243). IEEE.
66. Ali, A. K., & Bhaya, W. S. (2021, March). Detection of Misuse Attack in NFV Networks Using Machine Learning. In *Journal of Physics: Conference Series* (Vol. 1818, No. 1, p. 012123). IOP Publishing.
67. Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J. M., & Kim, D. S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. *Computer Networks*, *188*, 107871.
68. Anwer, H. M., Farouk, M., & Abdel-Hamid, A. (2018, April). A framework for efficient network anomaly intrusion detection with features selection. In *2018 9th International Conference on Information and Communication Systems (ICICS)* (pp. 157-162). IEEE.
69. Mozo, A., Pastor, A., Karamchandani, A., de la Cal, L., Rivera, D., & Moreno, J. I. (2022). Integration of Machine Learning-Based Attack Detectors into Defensive Exercises of a 5G Cyber Range. *Applied Sciences*, *12*(20), 10349.
70. Rezvani, M. (2018). Assessment methodology for anomaly-based intrusion detection in cloud computing. *Journal of AI and Data Mining*, *6*(2), 387-397.
71. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, *16*(1), 303-336.
72. Chauhan, S., & Vig, L. (2015, October). Anomaly detection in ECG time signals via deep long short-term memory networks. In *2015 IEEE international conference on data science and advanced analytics (DSAA)* (pp. 1-7). IEEE.
73. Chou, H. H., & Wang, S. D. (2015, September). An adaptive network intrusion detection approach for the cloud environment. In *2015 international carnahan conference on security technology (iCCST)* (pp. 1-6). IEEE.
74. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *Ieee Access*, *5*, 21954-21961.
75. Nazir, A., & Khan, R. A. (2019). Combinatorial optimization based feature selection method: A study on network intrusion detection. *arXiv preprint arXiv:1906.04494*.
76. Cotroneo, D., Natella, R., & Rosiello, S. (2017, October). A fault correlation approach to detect performance anomalies in virtual network function chains. In *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)* (pp. 90-100). IEEE.
77. Cruz, T., Rosa, L., Proença, J., Maglaras, L., Aubigny, M., Lev, L., ... & Simões, P. (2016). A cybersecurity detection framework for supervisory control and data acquisition systems. *IEEE Transactions on Industrial Informatics*, *12*(6), 2236-2246.
78. Dimolianis, M., Pavlidis, A., & Maglaris, V. (2021). Signature-based traffic classification and mitigation for ddos attacks using programmable network data planes. *IEEE Access*, *9*, 113061-113076.
79. Kazemi, S., Aghazarian, V., & Hedayati, A. (2015). Improving false negative rate in hypervisor-based intrusion detection in IaaS cloud. *IJCAT Int. J. Comput. Technol*, *2*(9), 348.
80. Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction. *Entropy*, *15*(6), 2218-2245.
81. Farnaaz, N., & Jabbar, M. A. (2016). Random forest modeling for network intrusion detection system. *Procedia Computer Science*, *89*, 213-217.
82. Moustafa, N., Keshky, M., Debiez, E., & Janicke, H. (2020, December). Federated TON_IoT Windows datasets for evaluating AI-based security applications. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 848-855). IEEE.
83. Gamal, M., Abbas, H. M., Moustafa, N., Sitnikova, E., & Sadek, R. A. (2021). Few-shot learning for discovering anomalous behaviors in edge networks. *Computers, Materials and Continua*, *69*(2), 1823-1837.
84. Alnaim, A. K. (2022). Misuse Patterns from the Threat of Modification of Non-Control Data in Network Function Virtualization. *Future Internet*, *14*(7), 201.
85. Bhardwaj, A., Mangat, V., & Vig, R. (2020). Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. IEEE Access, 8, 181916-181929.
86. Gandhi, K., & Qaddour, J. (n.d.). Implementation Problems Facing Network Function Virtualization and Solutions.
87. Idhammad, M., Afdel, K., & Belouch, M. (2018). Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Computer Science, 127, 35-41.
88. Li, J., Zhao, Z., & Li, R. (2018). Machine learning-based IDS for software-defined 5G network. Iet Networks, 7(2), 53-60.
89. Dhaliwal, S. S., Nahid, A. A., & Abbas, R. (2018). Effective intrusion detection system using XGBoost. Information, 9(7), 149.
90. Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2021). Machine learning towards intelligent systems: applications, challenges, and opportunities. Artificial Intelligence Review, 54, 3299-3348.
91. Aiken, J., & Scott-Hayward, S. (2019, November). Investigating adversarial attacks against network intrusion detection

systems in sdns. In 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 1-7). IEEE.
92. Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2017, January). Malware traffic classification using convolutional neural network for representation learning. In 2017 International conference on information networking (ICOIN) (pp. 712-717). IEEE.
93. Thang, N. C., & Park, M. (2020). Detecting Malicious Middleboxes In Service Function Chaining. J. Internet Serv. Inf. Secur., 10(2), 82-90.
94. Koc, L., Mazzuchi, T. A., & Sarkani, S. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. Expert Systems with Applications, 39(18), 13492-13500.
95. Lavin, A., & Ahmad, S. (2015, December). Evaluating real-time anomaly detection algorithms--the Numenta anomaly benchmark. In 2015 IEEE 14th international conference on machine learning and applications (ICMLA) (pp. 38-44). IEEE.
96. Leu, F. Y., Tsai, K. L., Hsiao, Y. T., & Yang, C. T. (2015). An internal intrusion detection and protection system by using data mining and forensic techniques. IEEE Systems Journal, 11(2), 427-438.
97. Tian, Z., Cui, Y., An, L., Su, S., Yin, X., Yin, L., & Cui, X. (2018). A real-time correlation of host-level events in cyber range service for smart campus. IEEE Access, 6, 35355-35364.
98. Lu, H., Li, Y., Mu, S., Wang, D., Kim, H., & Serikawa, S. (2017). Motor anomaly detection for unmanned aerial vehicles using reinforcement learning. IEEE internet of things journal, 5(4), 2315-2322.
99. Modi, C. N., & Acha, K. (2017). Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. the Journal of Supercomputing, 73(3), 1192-1234.
100. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 25(1-3), 18-31.
101. Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE access, 6, 48231-48246.
102. Wang, Z., Liu, Y., He, D., & Chan, S. (2021). Intrusion detection methods based on integrated deep learning model. Computers & Security, 103, 102177.
103. Shareena, J., Ramdas, A., & AP, H. (2021). Intrusion detection system for iot botnet attacks using deep learning. SN Computer Science, 2(3), 205.
104. Youssef, A., & Emam, A. (2011). Network intrusion detection using data mining and network behaviour analysis. International journal of computer science & information technology, 3(6), 87.
105. Peiravian, N., & Zhu, X. (2013, November). Machine learning for android malware detection using permission and api calls. In 2013 IEEE 25th international conference on tools with artificial intelligence (pp. 300-305). IEEE.
106. Razdan, S., Gupta, H., & Seth, A. (2021, April). Performance analysis of network intrusion detection systems using j48 and naive bayes algorithms. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-7). IEEE.
107. de Miranda Rios, V., Inácio, P. R., Magoni, D., & Freire, M. M. (2021). Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. Computer Networks, 186, 107792.
108. Sauvanaud, C., Lazri, K., Kaâniche, M., & Kanoun, K. (2016, October). Anomaly detection and root cause localization in virtual network functions. In 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE) (pp. 196-206). IEEE.
109. Sauvanaud, C., Lazri, K., Kaâniche, M., & Kanoun, K. (2016, June). Towards black-box anomaly detection in virtual network functions. In 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W) (pp. 254-257). IEEE.
110. Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. Sensors, 19(9), 1977.
111. Alsharif, M., & Rawat, D. B. (2021). Study of machine learning for cloud assisted iot security as a service. Sensors, 21(4), 1034.
112. Zhong, M., Zhou, Y., & Chen, G. (2021). Sequential model based intrusion detection system for IoT servers using deep learning methods. Sensors, 21(4), 1113.
113. Song, C., Park, Y., Golani, K., Kim, Y., Bhatt, K., & Goswami, K. (2017, July). Machine-learning based threat-aware system in software defined networks. In 2017 26th international conference on computer communication and networks (ICCCN) (pp. 1-9). IEEE.
114. Soni, S., & Bhushan, B. (2019, July). Use of Machine Learning algorithms for designing efficient cyber security solutions. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (Vol. 1, pp. 1496-1501). IEEE.
115. Stroeh, K., Mauro Madeira, E. R., & Goldenstein, S. K. (2013). An approach to the correlation of security events based on machine learning techniques. Journal of Internet Services and Applications, 4, 1-16.
116. Aboueata, N., Alrasbi, S., Erbad, A., Kassler, A., & Bhamare, D. (2019, July). Supervised machine learning techniques for efficient network intrusion detection. In 2019 28th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-8). IEEE.

Conflict of Interest Notice
The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical Approval and Informed Consent
It is declared that during the preparation process of this study, scientific and ethical principles were followed, and all the studies benefited from are stated in the bibliography.

Availability of data and material
Not applicable.

Plagiarism Statement
This article has been scanned by iThenticate ™.