Research Article

ACCENTS Transactions on Information Security, Vol 7(28)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2022.725014

Enhancing network security: ACO-KM algorithm for intrusion detection

Ashvin Subhashchandra Pandey* **and Mohan Kumar Patel**
School of Computer Science and Engineering, Madhyanchal Professional University, Bhopal, India

Received: 14-July-2022; Revised: 05-October-2022; Accepted: 10-October-2022

Abstract

In today's world, ensuring the security and integrity of networks is of utmost importance. With the evolving digital landscape, malicious actors employ increasingly sophisticated tactics to gain unauthorized access to sensitive information. Intrusion Detection Systems (IDSs) are pivotal in safeguarding networks by identifying abnormal activities or intrusions. Traditional rule-based IDSs have limitations in detecting evolving threats, leading to the emergence of machine learning-based approaches. This paper explores the integration of Ant Colony Optimization (ACO) and K-means clustering (ACO-KM) to enhance intrusion detection on the NSL-KDD dataset, addressing the need for adaptive IDSs capable of identifying emerging threats. The paper presents a comprehensive literature review, details the ACO-KM algorithm, and evaluates intrusion detection performance. The approach is implemented using NETBEANS IDE and provides flexibility in data selection and classification. Results indicate superior accuracy in detecting Denial of Service (DoS) attacks, emphasizing the efficacy of the proposed ACO-KM algorithm in bolstering network security.

Keywords

Intrusion detection, Network security, Ant colony optimization, NSL-KDD dataset.

1.Introduction

In today's digitally interconnected world, where data is constantly being transmitted across networks, ensuring the security and integrity of these networks is of paramount importance [1, 2]. As the digital landscape continues to evolve, so do the tactics employed by malicious actors seeking unauthorized access to sensitive information. Intrusion detection systems (IDSs) play a pivotal role in safeguarding networks by monitoring and identifying abnormal activities or intrusions [3–5].

The proliferation of the internet and the ubiquity of networked systems have revolutionized the way individuals and organizations interact and transact [6, 7]. However, this digital revolution has also exposed these networks to an array of security threats [8, 9]. IDSs, conceived as a response to this ongoing threat landscape, have evolved to become indispensable components of network security [10, 11].

Traditional rule-based IDSs rely on predefined patterns to detect known attacks [12–16]. While effective in some scenarios, they often fall short when faced with previously unseen or evolving threats. Machine learning-based IDSs offer a more adaptive and proactive approach. [17, 18] These systems leverage the power of data to learn and recognize patterns indicative of intrusions. One crucial step in this process is the availability of comprehensive and diverse datasets for training and evaluation.

The NSL-KDD dataset, an improved version of the widely used KDD'99 dataset, has emerged as a benchmark dataset in the field of intrusion detection [19, 20]. It addresses some of the limitations of its predecessor, including the removal of duplicate and redundant records. Its multi-class nature encompasses various attack categories, making it an ideal choice for evaluating IDSs in real-world scenarios [18–20].

The motivation behind this research stems from the ever-increasing sophistication of cyber threats. Attackers are continually devising novel techniques to evade traditional security measures. Therefore, there is a compelling need for IDSs that can adapt and learn from data, allowing them to detect not only known attacks but also emerging threats. Ant Colony Optimization (ACO), inspired by the foraging behavior of ants, has demonstrated its effectiveness

*Author for correspondence

in solving complex optimization problems. When applied to the realm of intrusion detection, ACO has the potential to enhance the accuracy and efficiency of anomaly detection. K-means clustering, on the other hand, is a powerful unsupervised learning technique that can be used to group network data into clusters, making it easier to identify abnormal patterns. Combining ACO with K-means clustering offers a promising avenue for improving the detection capabilities of IDSs.

The primary objective of this research is to apply ACO in conjunction with k-means-based clustering (ACO-KM) to detect intrusions on the NSL-KDD dataset. ACO has been used as a feature selection mechanism to identify the most relevant features for intrusion detection within the NSL-KDD dataset. K-means clustering has been applied to group network data into clusters based on the selected features.

This paper is organized as follows: Section 2 explores the review and analysis. Section 3 discusses the methods used. Results and discussions are elaborated in Section 4. Finally, the conclusion is presented in Section 5.

2.Literature review

In this literature review section, a thorough examination and analysis of the research concerning intrusion detection systems (IDS) have been elaborated. This analysis encompasses a comprehensive overview of the relevant academic work, aiming to provide a deeper understanding of the state-of-the-art in IDS research. We scrutinize various methodologies, techniques, and findings from prior studies to identify trends, strengths, weaknesses, and emerging areas of interest within the field of intrusion detection.

In 2022, Zhang et al. [21] explored machine learning algorithms in network intrusion detection, categorizing them as traditional, ensemble, and deep learning. Ensemble learning outperformed, while Naive Bayes excelled at new attacks but lacked accuracy on familiar ones. Deep learning's effectiveness depended on architecture and hyperparameters. They also highlighted challenges and future research directions.

In 2022, Balyan et al. [22] developed a hybrid network-based Intrusion Detection System (HNIDS) to address data imbalance issues in machine learning-based IDS. Their HNIDS achieved impressive accuracy, outperforming traditional ML methods on the NSL-KDD dataset.

In 2022, Ullah et al. [23] addressed the need for secure online communication during the COVID-19 pandemic. They proposed an intrusion detection system for Apache web servers, using the Naive Bayes algorithm for training. Their system achieved a high cross-validation accuracy of 98.6% using an IEEE dataset.

In 2022, Saba et al. [24] emphasized the critical security challenges posed by the Internet of Things (IoT) and the need for advanced security measures. They proposed a CNN-based anomaly-based Intrusion Detection System (IDS) for IoT, achieving impressive accuracy of 99.51% on NID Dataset and 92.85% on BoT-IoT datasets.

In 2022, Liu et al. [25] addressed wireless sensor network security through edge computing, introducing a WSN intrusion detection model combining k-Nearest Neighbor and arithmetic optimization (AOA). Their model achieved 99% accuracy, particularly effective against DoS attacks.

In 2022, Fu et al. [26] recognized the limitations of traditional network security methods and proposed DLNID, a deep learning-based model for traffic anomaly detection. DLNID demonstrated superior accuracy (90.73%) and F1 score (89.65%) on the NSL-KDD dataset.

In 2022, Saheed et al. [27] highlighted the growing importance of securing IoT devices and proposed an ML-based IDS for IoT network attacks. Their model achieved remarkable accuracy (99.9%) and MCC (99.97%) on the UNSW-NB15 dataset.

In 2022, Mushtaq et al. [28] tackled the challenges of intrusion detection system design, introducing a hybrid AE-LSTM model that significantly outperformed other techniques with an accuracy of 89% on NSL-KDD.

In 2022, Wahab [29] addressed data and concept drift in IoT-based IDS with an adaptive online deep neural network (DNN) solution, stabilizing performance over time in dynamic IoT environments.

In 2023, Thakkar and Lohiya [30] focused on enhancing DNN-based IDS with a novel feature selection technique based on statistical importance fusion, achieving competitive results across multiple intrusion detection datasets and considering execution time and statistical significance.

3.Method

The ACO-KM Algorithm for IDS combines Ant Colony Optimization (ACO) with K-means clustering to enhance intrusion detection capabilities. It begins by initializing essential parameters and empty clusters, followed by a main loop where a population of ants iteratively selects features using ACO and applies K-means clustering to evaluate fitness. Pheromone levels are updated based on fitness, and the loop continues until convergence or the maximum iteration limit is reached. Afterward, a final K-means clustering step is performed on selected features to obtain clusters, and intrusion detection performance metrics are evaluated. The algorithm outputs the chosen features, resulting clusters, and performance metrics, offering an effective approach to adaptively identify intrusions in network data. The dataset considerd was NSL-KDD dataset.

This approach has been developed within the NETBEANS IDE environment, supported by JDK version 7 or higher. It provides the flexibility to choose between random data selection or processing the entire dataset simultaneously. For experimental purposes, random data selection has been employed to facilitate comparisons with previous research. However, it's worth noting that there is also an option to select and process all the data at once. The data can be classified either individually or as a group, allowing for various analysis methods. *Figure 1* shows the complete flowchart of the approach.

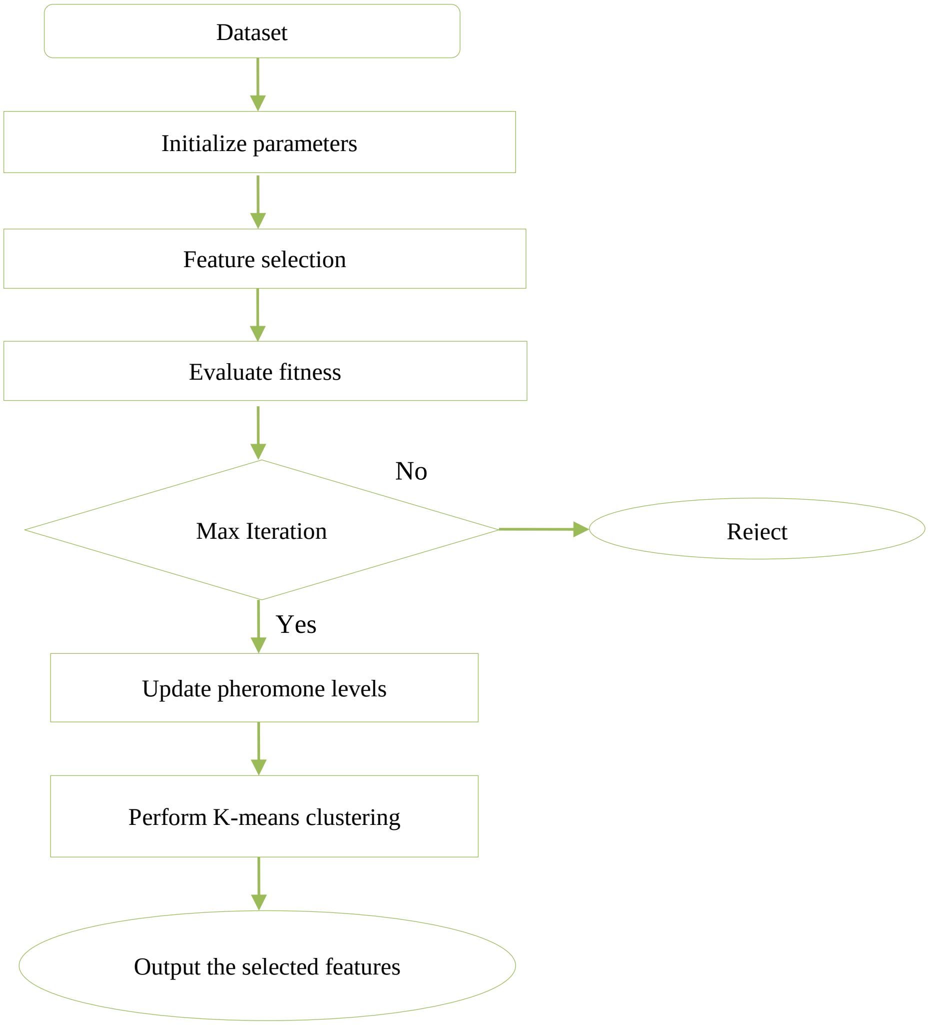

Figure 1 Flowchart of ACO-KM based system

Algorithm: ACO-KM Algorithm for Intrusion Detection System

```
Initialization:
    1. Initialize pheromone levels on all features.
    2. Initialize parameters (e.g., number of ants,
       max iterations, alpha, beta).
    3. Initialize K-means parameters (e.g., number
       of clusters, convergence threshold).
    4. Initialize empty clusters.

Main Loop:
    5. For each iteration in the range of
       max_iterations:
       Create a population of ants.
            For each ant in the range of
       num_ants:
Feature selection using ACO.
selected_features =
select_features_with_aco(pheromone_levels)
Apply K-means clustering.
clusters = k_means_clustering(selected_features,
num_clusters)
Evaluate fitness of clusters.
fitness = evaluate_clusters(clusters)
Update pheromone levels based on fitness.
update_pheromone(pheromone_levels,
selected_features, fitness)
Check for convergence or max iterations.
If convergence_criteria_met() or iteration==
max_iterations, then exit the loop.
Final Clustering:
    6. Perform K-means clustering on the selected
       features to obtain the final clusters.
       clusters=
k_means_clustering(selected_features, num_clusters)

Evaluate Intrusion Detection Performance:
    7. Evaluate intrusion detection performance
       metrics (e.g., accuracy, F1-score) using the
       final clusters.
       performance_metrics=
evaluate_intrusion_detection(clusters)

Output:
    8. Output the selected features, clusters, and
       performance metrics.

End
```

4.Results

In this paper, we have specifically focused our analysis on the results of Denial of Service (DoS) attacks. We have examined the performance of our approach in detecting various types of DoS attacks, including Back, Land, Neptune, Smurf, Teardrop, and Pod. The corresponding percentages derived from our dataset are illustrated in *Figure 2*. The results unequivocally demonstrate that our approach exhibits superior accuracy in detecting these attacks, as indicated by the successful identification of a significant majority of them, as illustrated in *Figure 3*.

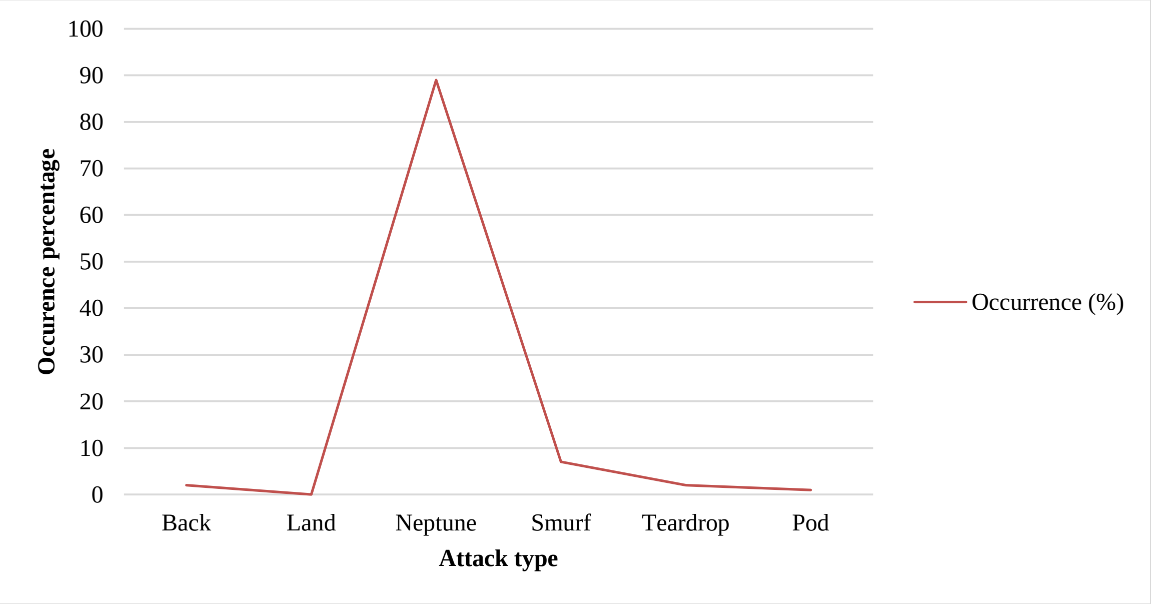

Figure 2 Occurrence percentage in the complete dataset

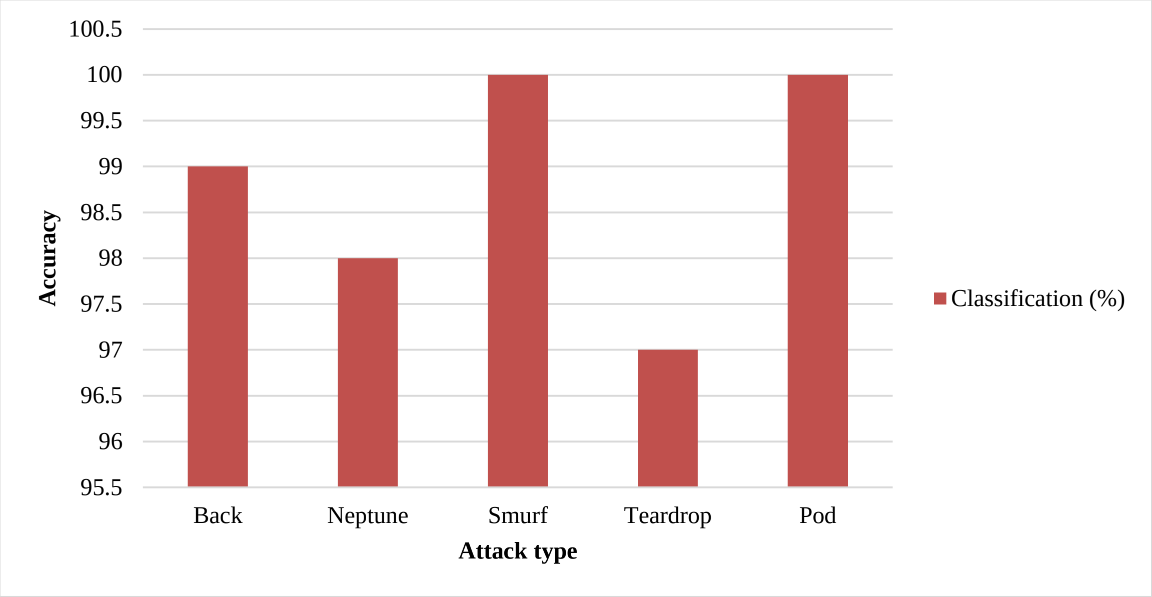

Figure 2 Occurrence percentage in the complete dataset

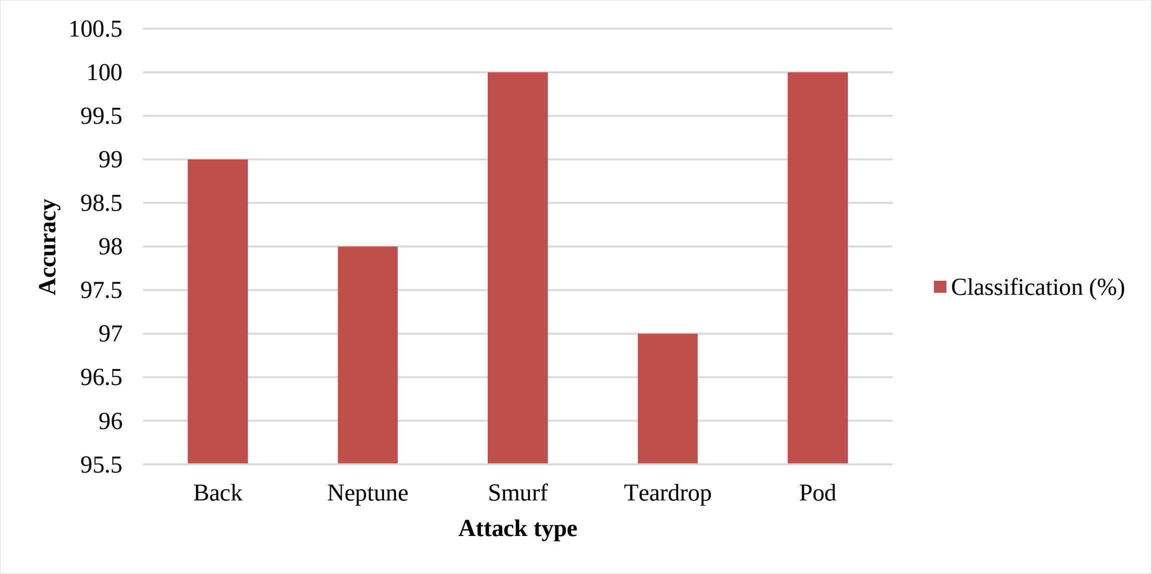

Figure 3

5.Conclusion

In an era defined by digital connectivity, safeguarding networks against evolving cyber threats is paramount. This paper introduces the ACO-KM Algorithm for Intrusion Detection, which combines Ant Colony Optimization and K-means clustering to enhance network security. The approach's adaptability and effectiveness are demonstrated through the detection of various Denial of Service attacks. Leveraging the NSL-KDD dataset, our approach showcases remarkable accuracy in identifying these threats, underlining its potential to fortify network defenses in today's digitally transformed landscape. As network threats continue to evolve, the ACO-KM Algorithm offers a promising avenue to ensure the security and integrity of our interconnected networks.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Liao HJ, Lin CH, Lin YC, Tung KY. Intrusion detection system: a comprehensive review. Journal of Network and Computer Applications. 2013; 36(1):16-24.

[2] Heidari A, Jabraeil Jamali MA. Internet of things intrusion detection systems: a comprehensive review and future directions. Cluster Computing. 2022:1-28.

[3] Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019; 2(1):1-22.

[4] Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S. Deep learning approach for intelligent intrusion detection system. IEEE Access. 2019; 7:41525-50.

[5] Sasubilli SM, Dubey AK, Kumar A. A computational and analytical approach for cloud computing security with user data management. In international conference on advances in computing and communication engineering (ICACCE) 2020 (pp. 1-5). IEEE.

[6] Ahmad Z, Shahid Khan A, Wai Shiang C, Abdullah J, Ahmad F. Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 2021; 32(1):e4150.

[7] Smys S, Basar A, Wang H. Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC. 2020; 2(04):190-9.

[8] Saranya T, Sridevi S, Deisy C, Chung TD, Khan MA. Performance analysis of machine learning algorithms in intrusion detection system: a review. Procedia Computer Science. 2020; 171:1251-60.

[9] Albulayhi K, Abu Al-Haija Q, Alsuhibany SA, Jillepalli AA, Ashrafuzzaman M, Sheldon FT. IoT intrusion detection using machine learning with a novel high performing feature selection method. Applied Sciences. 2022; 12(10):5015.

[10] Vijay A, Patidar K, Yadav M, Kushwah R. An analytical survey on the role of machine learning algorithms in case of intrusion detection. ACCENTS Transactions on Information Security. 2020; 5 (19): 32-35.

[11] Naseri TS, Gharehchopogh FS. A feature selection based on the farmland fertility algorithm for improved intrusion detection systems. Journal of Network and Systems Management. 2022; 30(3):40.

[12] Ferdiana R. A systematic literature review of intrusion detection system for network security: Research trends, datasets and methods. In 4th international conference on informatics and computational sciences (ICICoS) 2020 (pp. 1-6). IEEE.

[13] Kopecky S, Dwyer C. Nature inspired metaheuristic techniques of firefly and grey wolf algorithms implemented in phishing intrusion detection systems. In science and information conference 2023 (pp. 1309-32). Cham: Springer Nature Switzerland.

[14] GSR ES, Azees M, Vinodkumar CR, Parthasarathy G. Hybrid optimization enabled deep learning technique for multi-level intrusion detection. Advances in Engineering Software. 2022; 173:103197.

[15] Kumar A, Kumar SA, Dutt V, Kumar Dubey A, Narang S. A hybrid secure cloud platform maintenance based on improved attribute-based encryption strategies. International Journal of Interactive Multimedia and Artificial Intelligence. 2023; 8(2): 150-157.

[16] Hassan IH, Mohammed A, Masama MA. Metaheuristic algorithms in network intrusion detection. Comprehensive Metaheuristics. 2023:95-129.

[17] Liu Z, Xu B, Cheng B, Hu X, Darbandi M. Intrusion detection systems in the cloud computing: a comprehensive and deep literature review. Concurrency and Computation: Practice and Experience. 2022; 34(4):e6646.

[18] Almasoud AS. Intelligent deep learning enabled wild forest fire detection system. Computer Systems Science & Engineering. 2023; 44(2).

[19] Duhayyim MA, Alissa KA, Alrayes FS, Alotaibi SS, Tag El Din EM, Abdelmageed AA, et al. Evolutionary-based deep stacked autoencoder for intrusion detection in a cloud-based cyber-physical system. Applied Sciences. 2022; 12(14):6875.

[20] Maldonado J, Riff MC, Neveu B. A review of recent approaches on wrapper feature selection for intrusion detection. Expert Systems with Applications. 2022; 198:116822.

[21] Zhang C, Jia D, Wang L, Wang W, Liu F, Yang A. Comparative research on network intrusion detection methods based on machine learning. Computers & Security. 2022: 102861.

[22] Balyan AK, Ahuja S, Lilhore UK, Sharma SK, Manoharan P, Algarni AD, et al. A hybrid intrusion detection model using ega-pso and improved random forest method. Sensors. 2022; 22(16):5986.

[23] Ullah MU, Hassan A, Asif M, Farooq MS, Saleem M. Intelligent intrusion detection system for apache web server empowered with machine learning approaches. International Journal of Computational and Innovative Sciences. 2022; 1(1):21-7.

[24] Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering. 2022; 99:107810.

[25] Liu G, Zhao H, Fan F, Liu G, Xu Q, Nazir S. An enhanced intrusion detection model based on improved kNN in WSNs. Sensors. 2022; 22(4):1407.

[26] Fu Y, Du Y, Cao Z, Li Q, Xiang W. A deep learning model for network intrusion detection with imbalanced data. Electronics. 2022; 11(6):898.

[27] Saheed YK, Abiodun AI, Misra S, Holone MK, Colomo-Palacios R. A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal. 2022; 61(12):9395-409.

[28] Mushtaq E, Zameer A, Umer M, Abbasi AA. A two-stage intrusion detection system with auto-encoder and LSTMs. Applied Soft Computing. 2022; 121:108768.

[29] Wahab OA. Intrusion detection in the iot under data and concept drifts: Online deep learning approach. IEEE Internet of Things Journal. 2022; 9(20):19706-16.

[30] Thakkar A, Lohiya R. Fusion of statistical importance for feature selection in deep neural network-based intrusion detection system. Information Fusion. 2023; 90:353-63.

Mohan Kumar Patel is working as Assistant professor with the department of Computer Science and Engineering at Madhyanchal Proffessional University , Bhopal , India. He has completed his Bachelor of Engineering and Master of Technology in Computer Science Engineering from RGPV Technical University Bhopal (M.P). He has 1 publication and conferences. His reserch area in network and network security, cryptography etc.

Email: patel.mohan67@gmail.com