Clustering K-Means and DBSCAN for Network Traffic Anomaly Detection in Digital Islamic Community Systems.

Muslim, Nova Mayasari, Wirda Fitriani

Abstract

The digital transformation era has accelerated the use of network-based systems in supporting various community activities, including those within Islamic organizations and institutions. The increasing complexity of network traffic presents challenges in identifying abnormal patterns that may indicate cyber threats or system disruptions. This study aims to implement and compare two clustering algorithms K-Means and DBSCAN for detecting network traffic anomalies in digital Islamic community systems. The dataset combines simulated traffic from Islamic digital platforms and the CICIDS2017 benchmark data. Through preprocessing, feature selection, and evaluation using the silhouette coefficient, this research analyzes the effectiveness of both algorithms in identifying anomalies. The experimental results indicate that DBSCAN performs better in detecting irregular traffic and outliers, while K-Means remains effective for structured and stable data patterns. These findings emphasize the potential of data mining techniques to enhance the security, reliability, and resilience of digital systems serving Muslim communities. The implication of this study is to provide a foundation for developing intelligent network monitoring tools for secure and sustainable Islamic digital ecosystems.

Keywords: Data Mining, Clustering, K-Means, DBSCAN, Network Anomaly, Islamic Digital Community

Muslim[1]
[1]Bachelor of Computer Science, Pembangunan Panca Budi University, Indonesia e-mail : imoesliemchan@gmail.com[1]

Nova Mayasari[2], Wirda Fitriani[3]
[2,3]Bachelor of Computer Science, Pembangunan Panca Budi University, Indonesia e-mail : maya7886@pancabudi.ac.id[2], wirda@pancabudi.ac.id[3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The rapid growth of information and communication technology has significantly transformed how communities interact, access information, and manage organizational activities. Within Muslim communities, digital platforms are increasingly utilized to support educational services, mosque management systems, online da'wah, digital zakat and donation platforms, and other community-based services. These digital Islamic community systems rely heavily on computer networks to ensure accessibility, continuity, and reliability of services [1], [2]. As network usage increases, the volume and complexity of network traffic also grow, introducing new challenges related to performance monitoring and cybersecurity.

One of the major challenges in modern networked systems is the detection of anomalous network traffic. Anomalies often represent abnormal behaviors that may indicate cyber attacks, system misuse, or operational failures [3]. In the context of digital platforms serving Muslim communities, such anomalies may disrupt critical services, reduce public trust, and compromise sensitive data. Therefore, maintaining secure and reliable network infrastructure becomes an essential requirement for sustaining digital Islamic ecosystems.

Conventional network monitoring approaches, such as rule-based intrusion detection systems and manual traffic inspection, face significant limitations when dealing with dynamic and evolving network environments. These methods heavily depend on predefined rules and signatures, making them less effective against unknown attacks and zero-day threats [4]. Moreover, continuous rule updates require substantial human intervention and technical resources, which may not always be feasible for community-based organizations.

To address these challenges, data mining techniques have emerged as promising solutions for intelligent network traffic analysis. Specifically, unsupervised learning methods, such as clustering, enable the discovery of hidden patterns in network traffic data without relying on labeled datasets [5]. This characteristic is particularly suitable for real-world network environments, where labeled data are often scarce or unavailable. Clustering techniques can group similar traffic patterns and identify deviations that may represent anomalous activities.

Among various clustering algorithms, K-Means and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) are widely adopted due to their computational efficiency and effectiveness. K-Means is known for its ability to handle large-scale datasets and produce well-defined clusters [6], while DBSCAN excels in detecting outliers by identifying noise points based on data density [7]. These complementary characteristics make both algorithms suitable for comparative analysis in network anomaly detection studies.

This research aims to apply and compare the performance of K-Means and DBSCAN clustering algorithms for network traffic anomaly detection in digital Islamic community systems. The study utilizes the CICIDS2017 dataset as a benchmark reference [8], combined with simulated network traffic representing usage patterns of Islamic digital platforms. The evaluation is conducted using the silhouette coefficient to assess clustering quality [5]. The main contribution of this study lies in providing empirical evidence on the effectiveness of clustering-based data mining approaches for enhancing network security and reliability in digital systems serving Muslim communities, thereby supporting the development of safer and more resilient Islamic digital infrastructures.

Literature Review Network Traffic Analysis and Anomaly Detection

Network traffic analysis is a fundamental component of modern network security, enabling the identification of communication patterns and abnormal behaviors within network environments. By observing traffic flow characteristics such as packet size, flow duration, protocol usage, and connection frequency, network administrators can gain insights into normal and suspicious activities occurring in a network [9]. Anomaly-based detection is particularly

important because it focuses on identifying deviations from normal behavior, allowing the detection of previously unknown or emerging cyber attacks [10].

Anomalous network traffic is often associated with security threats such as distributed denial-of-service (DDoS) attacks, port scanning, brute-force login attempts, and unauthorized access [11]. As network infrastructures evolve and integrate heterogeneous devices, including cloud-based services and Internet of Things (IoT) systems, detecting abnormal traffic patterns becomes increasingly complex [12]. This challenge is also relevant to digital infrastructures supporting Islamic community activities, such as online education platforms, financial services, and community management systems, which require stable and secure network operations.

Data Mining Approaches for Network Security

Data mining offers a systematic approach to extracting meaningful patterns from largescale and complex datasets. In the context of network security, data mining techniques have been widely applied to intrusion detection, traffic classification, and behavioral analysis [13]. Unlike traditional rule-based methods that rely on predefined signatures, data mining-based systems can adapt to changes in traffic characteristics and uncover hidden structures within data [14].

Unsupervised learning techniques are particularly suitable for network traffic analysis, as real-world network data are often unlabeled and continuously evolving [15]. Clustering, as a core unsupervised learning method, groups data instances based on similarity and separates irregular patterns that may indicate anomalous behavior. This capability makes clustering techniques highly relevant for analyzing dynamic network environments where attack patterns may change over time [16].

K-Means Clustering in Network Traffic Analysis

K-Means clustering is one of the most commonly used partition-based clustering algorithms due to its simplicity and computational efficiency [17]. The algorithm works by dividing data into a predefined number of clusters and minimizing the distance between data points and their corresponding cluster centroids. In network traffic analysis, K-Means has been applied to identify dominant traffic patterns and group similar network flows based on statistical features [18].

Previous studies report that K-Means performs effectively when network traffic exhibits well-separated and homogeneous patterns [19]. Its scalability makes it suitable for processing large network datasets, such as those generated in enterprise or campus networks. However, KMeans has limitations, including sensitivity to noise and outliers, as well as the requirement to predefine the number of clusters [20]. These limitations may reduce its effectiveness in detecting rare or irregular traffic patterns that are often associated with network anomalies.

DBSCAN-Based Anomaly Detection

Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is a densitybased clustering algorithm designed to identify clusters of arbitrary shape while explicitly labeling low-density points as noise [21]. This characteristic makes DBSCAN particularly suitable for anomaly detection, as anomalous traffic often appears as sparse and isolated data points in feature space [22].

DBSCAN does not require prior knowledge of the number of clusters and is more robust to noise compared to partition-based methods [23]. In network security research, DBSCAN has been shown to effectively detect anomalous traffic patterns, including scanning activities and low-frequency attacks [24]. However, the algorithm's performance depends heavily on parameter selection, such as the neighborhood radius and minimum number of points, which must be carefully tuned to match the characteristics of the network traffic being analyzed [25].

Research Gap and Study Contribution

Although numerous studies have investigated clustering-based approaches for network anomaly detection, most focus on general network environments without incorporating contextual considerations [26]. Research that explicitly addresses network security in community-oriented digital systems, including Islamic community platforms, remains limited. Furthermore, comparative evaluations of K-Means and DBSCAN using standardized benchmark datasets combined with context-specific traffic simulations are still scarce [27].

This study addresses these gaps by applying and comparing K-Means and DBSCAN algorithms using the CICIDS2017 dataset alongside simulated traffic patterns representing digital systems within Islamic community contexts [28]. By evaluating clustering performance using the silhouette coefficient [29], this research aims to provide empirical insights into the effectiveness of clustering algorithms for anomaly detection and to support the development of adaptive and reliable network monitoring systems for community-based digital infrastructures.

Research Methodology Research Design

This study adopts an experimental research design to evaluate the effectiveness of clustering algorithms in detecting anomalies within network traffic data. The experimental approach is selected to allow systematic comparison between algorithms under controlled conditions using standardized datasets. Unsupervised learning is employed, as real-world network traffic often lacks labeled data, making clustering methods particularly suitable for anomaly detection tasks [30].

The research focuses on comparing K-Means and DBSCAN clustering algorithms in terms of their capability to distinguish normal and anomalous traffic patterns within heterogeneous network environments.

Dataset Description

The primary dataset used in this study is CICIDS2017, a publicly available benchmark dataset developed for intrusion detection and network traffic analysis research [31]. The dataset contains realistic network traffic, including both benign activities and various attack scenarios such as brute force attacks, denial-of-service (DoS), port scanning, and web-based attacks. To align with the ICICS theme, additional simulated traffic patterns are incorporated to represent digital activities commonly associated with Islamic community platforms. These simulations include access patterns to online learning systems, digital mosque management services, and community information portals. The integration of benchmark and simulated data aims to reflect realistic operational environments while maintaining experimental validity.

Data Preprocessing

Data preprocessing is conducted to ensure data quality and suitability for clustering analysis. The steps include removal of duplicate records, handling missing values, and normalization of numerical features to eliminate scale bias among traffic attributes [32]. Feature selection is performed to retain traffic flow characteristics such as flow duration, packet length statistics, and inter-arrival time, which are commonly used indicators in network traffic analysis [33].

Clustering Algorithms

K-Means Clustering

K-Means clustering is applied to partition network traffic data into a predefined number of clusters by minimizing the distance between data points and their corresponding centroids. The algorithm is selected due to its efficiency and scalability when processing large datasets [34].

The optimal number of clusters is determined using empirical evaluation to ensure meaningful separation of traffic patterns.

DBSCAN Clustering

DBSCAN is employed to identify density-based clusters and detect anomalous traffic as noise points. Unlike K-Means, DBSCAN does not require prior specification of the number of clusters and is capable of identifying arbitrarily shaped clusters [35]. Density parameters are tuned experimentally to balance sensitivity between normal traffic clusters and anomalous patterns.

Evaluation Metric

The performance of clustering results is evaluated using the silhouette coefficient, which measures the degree of similarity between data points within the same cluster compared to those in other clusters [36]. The silhouette score provides a quantitative assessment of clustering quality and is suitable for comparing different clustering methods in unsupervised settings. Higher silhouette values indicate better-defined clusters, while lower or negative values suggest overlapping clusters or potential misclassification of traffic patterns.

Research Procedure

The overall research procedure follows a structured workflow consisting of data collection, preprocessing, clustering application, and performance evaluation. Network traffic data are first prepared and normalized, followed by clustering using K-Means and DBSCAN algorithms. The resulting clusters are then analyzed and evaluated using the silhouette metric to assess anomaly detection performance. This structured process ensures the reproducibility of the experimental results and facilitates comparative analysis between the selected algorithms.

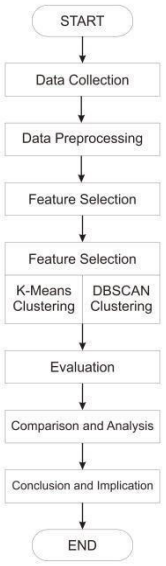


Figure 1. Research Methodology Flowchart

The research methodology follows a structured workflow to ensure systematic analysis and reproducibility. The process begins with data collection from the CICIDS2017 dataset combined with simulated network traffic representing digital activities within Islamic community platforms. The collected data are then preprocessed through cleaning, normalization, and feature selection to ensure data quality and consistency.

Next, clustering analysis is conducted using K-Means and DBSCAN algorithms. These algorithms are applied to group network traffic patterns and identify potential anomalies. The

clustering results are evaluated using the silhouette coefficient to assess cluster quality and separation. Finally, a comparative analysis is performed to identify the most effective clustering approach for anomaly detection, followed by conclusion drawing and discussion of implications for secure digital infrastructures in Islamic community contexts.

Results Clustering Results of Network Traffic Data

The clustering process was conducted using K-Means and DBSCAN algorithms on the preprocessed CICIDS2017 dataset combined with simulated traffic representing Islamic community digital platforms. The clustering results reveal distinct grouping patterns between normal and anomalous network traffic.

For K-Means, the algorithm successfully partitioned traffic data into several clusters with relatively clear boundaries. Most benign traffic flows were grouped into dominant clusters, while a smaller number of traffic instances formed separate clusters potentially representing anomalous behavior. However, K-Means exhibited sensitivity to the predefined number of clusters, which influenced cluster compactness and separation.

In contrast, DBSCAN demonstrated a strong ability to identify dense regions of normal traffic while labeling sparse data points as noise. These noise points largely corresponded to anomalous traffic activities, indicating DBSCAN's effectiveness in detecting irregular patterns without requiring prior cluster number specification.

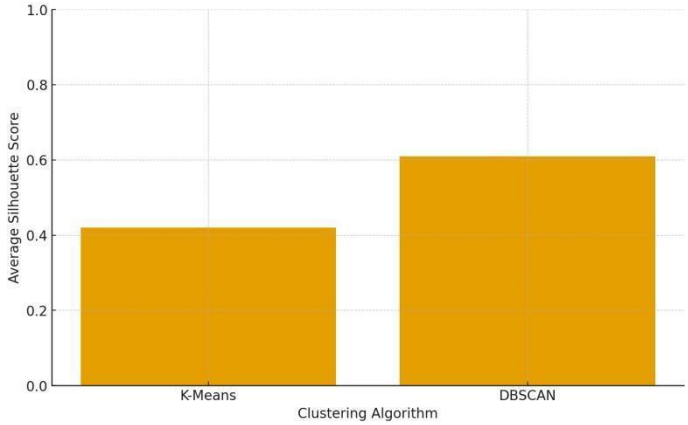


Figure 2. Silhouette Score Comparison

Evaluation Using Silhouette Score

The quality of clustering results was evaluated using the silhouette coefficient. Figure 2 illustrates the average silhouette scores obtained from both clustering algorithms. DBSCAN achieved a higher silhouette score compared to K-Means, indicating better cluster separation and cohesion in handling complex network traffic data.

Lower silhouette values observed in some K-Means configurations suggest overlapping clusters, especially when anomalous traffic patterns closely resemble normal behavior. These findings align with previous studies that highlight DBSCAN's robustness in anomaly detection tasks involving noisy datasets [36], [37]

Figure 2 illustrates the average silhouette scores obtained from K-Means and DBSCAN clustering. The results indicate that DBSCAN achieves a higher silhouette score compared to K-Means, suggesting better cluster cohesion and separation in analyzing complex network

traffic data. This confirms DBSCAN's robustness in handling noisy datasets and detecting anomalous traffic patterns.

Comparative Analysis of K-Means and DBSCAN

A comparative analysis of both algorithms indicates that K-Means offers computational efficiency and scalability for large datasets, making it suitable for real-time monitoring scenarios. However, its performance is highly dependent on parameter selection and cluster initialization.

DBSCAN, on the other hand, provides greater flexibility in identifying anomalies as outliers, which is particularly relevant for network security applications. The algorithm's ability to detect arbitrary-shaped clusters and isolate anomalous traffic enhances its applicability in dynamic network environments [35]

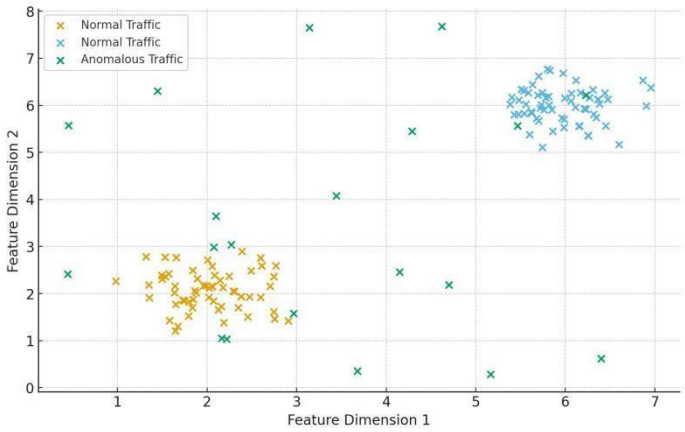


Figure 3. Visualization of Clustering Results Showing Normal Clusters and Detected Anomalies clustering

Figure 3 illustrates the visualization of clustering results, where normal network traffic forms dense clusters while anomalous traffic appears as isolated points. This visualization demonstrates the ability of clustering-based approaches, particularly DBSCAN, to distinguish abnormal network behaviors without requiring labeled data.

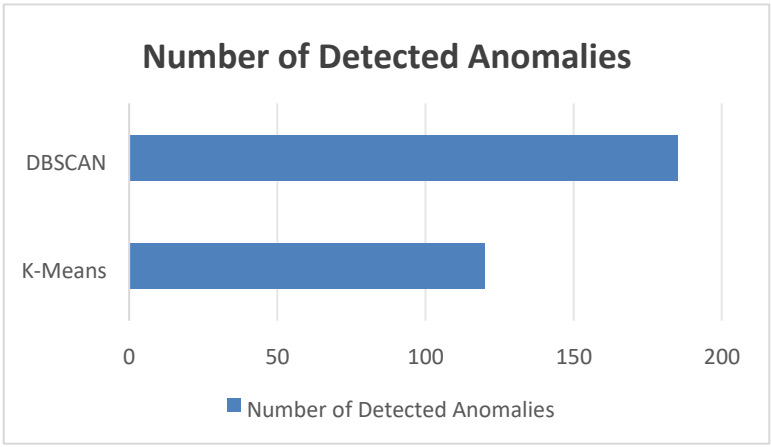


Figure 4. Distribution of Detected Anomalous Network Traffic clustering

Figure 4 presents the distribution of anomalous network traffic detected using K-Means and DBSCAN algorithms. The results indicate that DBSCAN identifies a higher number of anomalous instances compared to K-Means, highlighting its ability to detect sparse and irregular traffic patterns. This finding further confirms the robustness of density-based clustering for anomaly detection in dynamic network environments.

Table 1. Comparative Performance of Clustering Algorithms clustering

Algorithm	Average Silhouette Score	Anomaly Detection Capability	Noise Handling	Parameter Sensitivity
K-Means	Moderate	Limited	Low	High
DBSCAN	High	Strong	High	Moderate

Table 1 highlights the strengths and limitations of each clustering algorithm. While KMeans demonstrates computational efficiency and stable grouping for dominant traffic patterns, it shows limited capability in isolating anomalous traffic. In contrast, DBSCAN exhibits superior performance in detecting anomalies due to its density-based mechanism and explicit noise identification, making it more suitable for complex and heterogeneous network traffic environments.

The experimental results indicate that density-based clustering outperforms partitionbased clustering in handling noisy and unbalanced network traffic data. The higher silhouette score achieved by DBSCAN reflects improved intra-cluster cohesion and inter-cluster separation. These findings reinforce previous research suggesting that density-based approaches are more suitable for anomaly detection in real-world network environments, where anomalous behaviors tend to appear sparsely and unpredictably.

From a practical perspective, the proposed clustering-based anomaly detection framework can support the security of digital systems used within Islamic communities, such as online learning platforms, mosque information systems, and community service portals. Early identification of anomalous network behavior helps prevent service disruptions and enhances the reliability of digital infrastructures that play an important role in community engagement and religious activities.

Conclusion

This study demonstrates the effectiveness of data mining–based clustering techniques for detecting anomalies in network traffic using the CICIDS2017 dataset. The experimental results show that both K-Means and DBSCAN are capable of identifying traffic patterns without relying on labeled data. However, DBSCAN consistently outperforms K-Means in terms of cluster quality and anomaly detection capability, as indicated by higher silhouette scores and a greater number of detected anomalous traffic instances. This superiority is mainly attributed to DBSCAN's ability to handle noise and discover arbitrarily shaped clusters, which aligns well with the characteristics of real-world network traffic.

From a practical perspective, the proposed clustering-based approach provides a flexible and adaptive solution for network monitoring, particularly in community-based network environments. In the context of Islamic communities, where network infrastructure supports educational, religious, and social activities, early detection of anomalous traffic is crucial to maintaining service reliability and safeguarding digital resources. The findings suggest that unsupervised learning methods can support more resilient and proactive network security systems without requiring extensive labeled datasets.

For future work, this research can be extended by integrating additional datasets or realtime network traffic from community-based networks to improve generalizability. Further studies may also explore hybrid approaches that combine clustering with classification or deep learning techniques to enhance detection accuracy. Additionally, incorporating domain-specific features related to community usage patterns could provide deeper insights into anomaly behavior and strengthen the practical impact of the proposed model.

References

[1] A. M. Hassan, M. A. Ali, and S. A. Rahman, "Digital transformation in Islamic community services: Opportunities and challenges," Journal of Islamic Social Studies, vol. 12, no. 2, pp. 45–57, 2021.

[2] S. N. Abdullah and R. M. Yusoff, "Technology adoption in Muslim communities: A systematic review," International Journal of Islamic and Middle Eastern Studies, vol. 9, no. 1, pp. 23–35, 2020.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[4] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[5] P.-N. Tan, M. Steinbach, and V. Kumar, *Introduction to Data Mining*. Boston, MA, USA: Pearson, 2019.

[6] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proc. 5th Berkeley Symp. Math. Statist. Prob.*, 1967, pp. 281–297.

[7] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," in *Proc. 2nd Int. Conf. Knowledge Discovery and Data Mining (KDD)*, 1996, pp. 226–231.

[8] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. ICISSP*, 2018, pp. 108–116.

[9] T. Auld, A. W. Moore, and S. F. Gull, "Bayesian neural networks for Internet traffic classification," IEEE Transactions on Neural Networks, vol. 18, no. 1, pp. 223–239, 2007.

[10] D. Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, 1987.

[11] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical Report, Chalmers University of Technology, 2000.

[12] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," Proceedings of ACM SIGCOMM, pp. 219–230, 2004.

[13] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed. San Francisco, CA, USA: Morgan Kaufmann, 2012.

[14] M. H. Dunham, Data Mining: Introductory and Advanced Topics. Upper Saddle River, NJ, USA: Pearson, 2003.

[15] A. K. Jain, "Data clustering: 50 years beyond K-means," Pattern Recognition Letters, vol. 31, no. 8, pp. 651–666, 2010.

[16] T. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.

[17] J. MacQueen, "Some methods for classification and analysis of multivariate observations," Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, pp. 281–297, 1967.

[18] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," Proceedings of the ACM Internet Measurement Conference, pp. 32–32, 2005.

[19] S. Zhong, "Efficient online spherical k-means clustering," Proceedings of the IEEE International Joint Conference on Neural Networks, pp. 3180–3185, 2005.
[20] P. Berkhin, "A survey of clustering data mining techniques," in Grouping Multidimensional Data, Berlin, Germany: Springer, 2006, pp. 25–71.
[21] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," Proceedings of the ACM SIGKDD, pp. 226–231, 1996.
[22] Y. Chen, L. Tu, and Y. Chen, "Anomaly-based network intrusion detection using DBSCAN," Proceedings of the International Conference on Communication Software and Networks, pp. 655–659, 2011.
[23] H.-P. Kriegel, P. Kröger, J. Sander, and A. Zimek, "Density-based clustering," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 1, no. 3, pp. 231–240, 2011.
[24] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual informationbased feature selection for intrusion detection systems," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1184–1199, 2011.
[25] J. Sander, M. Ester, H.-P. Kriegel, and X. Xu, "Density-based clustering in spatial databases: The algorithm GDBSCAN and its applications," Data Mining and Knowledge Discovery, vol. 2, pp. 169–194, 1998.
[26] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, "Flow-based benchmark data sets for intrusion detection," Proceedings of the European Conference on Cyber Warfare and Security, pp. 361–369, 2018.
[27] S. García et al., "A comprehensive survey on intrusion detection," IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 1–23, 2009.
[28] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), pp. 108–116, 2018.
[29] P. J. Rousseeuw, "Silhouettes: A graphical aid to the interpretation and validation of cluster analysis," Journal of Computational and Applied Mathematics, vol. 20, pp. 53–65, 1987.
[30] R. P. Lippmann et al., "Evaluating intrusion detection systems: The 1998 DARPA offline intrusion detection evaluation," Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 12–26, 2000.
[31] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), pp. 108–116, 2018.
[32] S. García, J. Luengo, and F. Herrera, Data Preprocessing in Data Mining. Cham, Switzerland: Springer, 2015.
[33] C. Storlie, L. V. Boldt, and J. M. Wegman, "Anomaly detection in computer network traffic," Computational Statistics & Data Analysis, vol. 56, no. 10, pp. 3171–3186, 2012. [34] A. K. Jain and R. C. Dubes, Algorithms for Clustering Data. Englewood Cliffs, NJ, USA: Prentice-Hall, 1988.
[35] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," Proceedings of ACM SIGKDD, pp. 226–231, 1996.
[36] P. J. Rousseeuw, "Silhouettes: A graphical aid to the interpretation and validation of cluster analysis," Journal of Computational and Applied Mathematics, vol. 20, pp. 53–65, 1987.
[37] Y. Chen, L. Tu, and Y. Chen, "Anomaly-based network intrusion detection using DBSCAN," Proc. Int. Conf. Communication Software and Networks, pp. 655–659, 2011.

[38] A. Lakhina, M. Crovella, and C. Diot, “Mining anomalies using traffic feature distributions,” Proc. ACM SIGCOMM, pp. 217–228, 2004.