

Research Article



Unsupervised Gaussian Mixture Model (GMM)-based Malware Detection in IoT Networks

Hemant Narottam Chaudhari 

Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), G. H. Rasoni College of Engineering and Management, Pune, Maharashtra, 412207, India

*Corresponding Author

Hemant N. Chaudhari

✉ hemantch09@gmail.com

Received: 03 August 2026

Revised: 11 September 2026

Accepted: 21 September 2026

Published Online: 22 September 2026

Citation

H. N. Chaudhari, Unsupervised Gaussian Mixture Model (GMM)-based malware detection in IoT networks, *Journal of Cybersecurity and Intelligent Systems*, 2026, 1(1), 26503, <https://doi.org/10.64189/cis.26503>.

Open Access

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/), which permits the non-commercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as appropriate credit to the original author(s) and the source is given by providing a link to the Creative Commons License and changes need to be indicated if there are any. The images or other third-party material in this article are included in the article's Creative Commons License, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons License and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this License, visit: <https://creativecommons.org/licenses/by-nc/4.0/>

© The Author(s) 2026

Abstract

With the rapid rise of cyber threats, traditional signature-based security systems struggle to detect sophisticated attacks, particularly zero-day threats and evolving malware. Supervised learning methods show promise but rely heavily on labeled datasets, limiting their adaptability. This paper explores an unsupervised learning-based approach for malware and network anomaly detection using the IoT-23 dataset. Our method enhances cybersecurity by providing an adaptive and proactive defense mechanism, effectively identifying threats while minimizing false positives. Unsupervised learning models, such as clustering and probabilistic techniques, excel at detecting novel threats without prior knowledge. Their integration with real-time threat intelligence enhances response capabilities, making them valuable for enterprise security, cloud environments, and critical infrastructure protection. Implementing these models in security information and event management (SIEM) systems improves automated threat mitigation and reduces manual intervention and response time. Future research should focus on refining these models for large-scale deployments, integrating hybrid AI techniques, and strengthening cybersecurity resilience. By continuously evolving to counter emerging threats, unsupervised learning-based security solutions play a pivotal role in next-generation defense strategies.

Keywords: Cyber threat detection; Artificial intelligence in cybersecurity; Zero-day attack detection; Security resilience; Adaptive threat detection; Proactive cyber defense.

1. Introduction

In today's digital landscape, cyber threats are becoming increasingly sophisticated, rendering traditional signature-based detection systems less effective against previously unseen threats.^[1,2] The rapid evolution of malware and network attacks has motivated the development of more adaptive and intelligent security mechanisms.^[1,3] Machine learning and deep learning techniques have therefore been increasingly investigated for anomaly and intrusion detection.^[4,5]

In this paper, the use of the Gaussian mixture model (GMM) for malware and network anomaly detection is investigated. The GMM can support the detection of previously unseen or anomalous network behaviors when the learned probability distribution adequately represents normal traffic.^[6,7]

GMM clusters data points on the basis of their statistical properties, making it effective at distinguishing between legitimate and malicious network activities. By applying the GMM to a malware detection dataset, this research aims to evaluate its effectiveness in identifying anomalies, reducing false positives, and improving overall threat detection accuracy. The proposed approach offers a scalable and adaptive solution to improve cybersecurity defenses, ensuring that networks remain resilient against evolving threats.

With the increasing complexity of modern cyberattacks, traditional security frameworks often struggle to maintain real-time defense mechanisms. Many existing intrusion detection systems (IDSs) rely on predefined rules and signature-based approaches, making them ineffective against previously unseen malware variants. The use of probabilistic models such as the GMM enhances the ability to detect threats dynamically without the need for extensive manual updates. This adaptability is crucial in countering sophisticated attacks such as polymorphic malware and advanced persistent threats (APTs), which continuously evolve to evade conventional detection strategies. Future research may also explore the integration of GMM-based detection within cloud-based security architectures, enabling large-scale, distributed threat monitoring across networks.

Additionally, real-world implementation of GMM-based malware detection in security operations centers (SOCs) and enterprise environments could lead to enhanced automated response mechanisms. By linking probabilistic threat detection with threat intelligence platforms, cybersecurity professionals can gain deeper insights into attack vectors, thereby reducing incident response times and mitigating potential damage. As cybercriminals continue to employ more advanced evasion techniques, the development of adaptive, AI-driven security solutions such as the GMM becomes increasingly vital for safeguarding digital infrastructures.

The continuous evolution of such models will play a crucial role in defending against emerging cyber threats ensuring robust and resilient cybersecurity frameworks.

2. Background and related work

Traditional signature-based security systems struggle to detect evolving cyber threats, especially zero-day attacks. Supervised learning approaches are based on labeled data, limiting their adaptability. In contrast, unsupervised learning, such as the Gaussian mixture model (GMM), can identify anomalies in network traffic without the need for labeled datasets, making it a promising approach for malware detection. The GMM probabilistically models data distributions, allowing them to detect deviations from normal behavior. This flexibility makes them useful for cybersecurity, where attack patterns frequently change. Unlike rigid rule-based systems, the GMM adapts dynamically to new threats. This study aims to leverage the GMM's clustering capabilities to enhance network security. The goal is to improve threat detection accuracy while minimizing false positives.

Previous research has explored supervised and unsupervised machine learning for cybersecurity. Although supervised models such as decision trees and neural networks perform well on known threats, they fail against novel attacks. Unsupervised methods, including the GMM, have been effective at detecting anomalies by clustering network traffic. Studies using datasets such as Aposemat IoT-23 have demonstrated the ability of the GMM to distinguish between normal and malicious activity, strengthening its potential for real-time threat detection. Researchers have compared the GMM with other clustering algorithms such as k-means, highlighting its ability to handle overlapping data distributions. Some studies have integrated the GMM with real-time monitoring for improved performance. Recent advances focus on optimizing the GMM parameters to improve the detection accuracy. This research builds on these works by applying the GMM to detect malware in dynamic network environments.

Furthermore, research has looked at hybrid techniques that combine the GMM with deep learning models such as autoencoders and recurrent neural networks (RNNs) to improve detection capabilities. These hybrid strategies increase feature extraction by lowering false positives while remaining adaptable to new threats. In addition, cloud-based anomaly detection systems use the GMM to quickly handle massive amounts of network traffic, demonstrating its scalability for business cybersecurity applications. Future research intends to combine GMM and adversarial learning approaches to improve defenses against sophisticated attack schemes. This study extends on previous work by using the GMM to identify malware in dynamic network settings, resulting in resilient and scalable security

solutions.

3. Literature survey

The growing sophistication of malware and cyber threats has rendered traditional signature-based detection methods ineffective, necessitating the use of unsupervised deep learning approaches for enhanced security. Gaussian mixture models (GMMs), hidden Markov models (HMMs), autoencoders, and hybrid AI-based anomaly detection techniques have been explored to improve malware classification and intrusion detection. This section presents a review of existing research on unsupervised learning for malware detection, emphasizing GMM-based methodologies and their integration with deep learning models.

J. Zhao *et al.* investigated GMM-HMM models for malware classification and demonstrated the efficacy of probabilistic techniques in detecting zero-day threats and polymorphic malware. This study emphasizes the capacity of the GMM to cluster network events on the basis of statistical features, resulting in much higher detection accuracy than that of standard rule-based systems. However, the paper cautions that the GMM-HMM models need careful hyperparameter adjustment to prevent false positives in large-scale datasets.^[8]

Similarly, S. Bertrand *et al.* explored Bayesian Gaussian mixture models (BGMMs) for insider threat detection and demonstrated their ability to detect anomalous user behaviors in network environments. Unlike conventional approaches that rely on predefined attack signatures, the BGMM dynamically learns evolving patterns, making it more adaptable to APTs. This study suggests the integration of deep autoencoders with a GMM to enhance feature extraction and improve detection performance.^[9]

Y. Chen *et al.* developed a self-organizing map (SOM)-assisted deep autoencoder Gaussian mixture model (DAGMM) for intrusion detection. The model uses dimensionality reduction and probabilistic clustering to accurately detect both known and undiscovered malware strains. The results show that the DAGMM outperforms typical IDS models in terms of false positives and anomaly detection precision. However, computational complexity remains a concern, necessitating additional optimizations for real-time network monitoring.^[10]

A. Interrante and G. Alexander investigate GMM for dynamic malware clustering, emphasizing its benefits in identifying evasive threats and polymorphic malware. This paper emphasizes the necessity for hybrid methods, suggesting that integrating a GMM with RNNs or reinforcement learning techniques might increase detection ability.^[11]

Unsupervised learning has been widely investigated for anomaly and intrusion detection because it can reduce the dependence on manually labeled attack

data.^[3,4] Deep learning-based anomaly detection approaches have also been studied extensively for cybersecurity applications.^[5,12,13,14,15]

Zong *et al.* proposed a deep autoencoder Gaussian mixture model (DAGMM) for unsupervised anomaly detection. The approach combines dimensionality reduction through an autoencoder with Gaussian mixture modeling to estimate the probability distribution of the latent representations.^[6] Chen *et al.* further investigated a self-organizing map-assisted DAGMM approach for unsupervised intrusion detection and reported improvements over conventional DAGMM approaches.^[16]

Recent research has also investigated the direct application of the GMM to network traffic anomaly detection. Yu *et al.* proposed a GMM-based network traffic anomaly detection method that evaluates the likelihood of observations under a learned Gaussian mixture distribution.^[7] Zhang *et al.* proposed an intrusion detection approach that combines a stacked sparse autoencoder with an improved GMM to address high-dimensional network data and unsupervised detection challenges.^[17]

Deep learning-based anomaly detection has also been investigated specifically for IoT networks. Meidan *et al.* proposed N-BaIoT, a network-based anomaly detection approach that uses deep autoencoders to detect IoT botnet attacks.^[18] Other studies have investigated machine learning-based detection and analysis of IoT network attacks using specialized IoT datasets.^[19,20]

Collectively, these studies demonstrate the promise of unsupervised deep learning models, particularly the GMM, in improving malware detection systems. Research has shown that hybrid models that combine probabilistic clustering and deep learning architectures can improve detection accuracy, reduce false positives, and increase scalability.

4. Objective

4.1 Proposed system

The objective of this system is to develop an unsupervised learning-based malware detection framework that efficiently identifies cyber threats in IoT networks. The system is designed as follows:

4.2 Training phase

- **Data collection:** The system uses the Aposemat IoT-23 dataset, which contains labeled benign and malicious IoT network traffic, as the primary dataset for model development and evaluation.^[21] The IoT-23 dataset contains 23 network traffic scenarios, comprising 20 malware-infected IoT captures and 3 benign IoT traffic captures.^[21]
- **Data cleaning:** Raw data are cleaned to remove noise, inconsistencies, and irrelevant information.
- **Data processing:** The cleaned data are processed and

transformed into suitable features for machine learning.

- **Unsupervised model training:** The processed data are used to train an unsupervised machine learning model, which learns to identify patterns and anomalies in network behavior.
- **Model evaluation:** The trained model's performance is evaluated to ensure that it meets accuracy and effectiveness requirements.

4.3 Real-Time detection

- **Network analysis:** Live network traffic is monitored and analyzed in real time.
- **Trained model application:** The previously trained model is applied to live network data to detect anomalies.
- **Alert generation:** When potential malware is detected, the system generates alerts.

5. System architecture and design

5.1 Malware detection using the Gaussian mixture model (GMM)

The system architecture for malware detection using the Gaussian mixture model (GMM) consists of two primary phases: a training phase and real-time detection. Each phase plays a crucial role in ensuring accurate and adaptive malware detection. The architecture is designed to process large volumes of network traffic, identify malicious patterns, and provide actionable insights to enhance cybersecurity defenses. The overall system architecture is illustrated in Fig. 1.

- **Data collection:** The Aposemat IoT-23 dataset serves as the major source of network traffic data. This dataset contains a variety of benign and harmful behaviors, including botnet infections, port scanning, and distributed denial-of-service (DDoS) assaults. To improve model robustness, more datasets or real-time network traffic recordings might be included. By utilizing a variety of sources, the system provides flexibility to emerging threats and variations in assault patterns.
- **Data cleaning:** Prior to training, the dataset is carefully cleaned to remove duplicate entries, missing values, and inconsistencies. Any unnecessary characteristics, noisy data, or duplicate entries are eliminated to improve model performance. By guaranteeing that only high-quality and valuable data are used, cleaning the dataset reduces the processing overhead and increases the detection accuracy.
- **Data processing:** Important elements required for malware identification are extracted from the data after they have been cleaned and analyzed. Feature engineering is used to identify key network attributes such as packet sizes, connection durations, and protocol types. To ensure uniformity and prevent bias from disparate scales, the numerical data are standardized. Furthermore, to enable smooth machine learning model training, categorical variables, such as protocol names and port numbers, are converted into numerical representations.
- **Unsupervised model training:** Training is performed using a probabilistic clustering approach

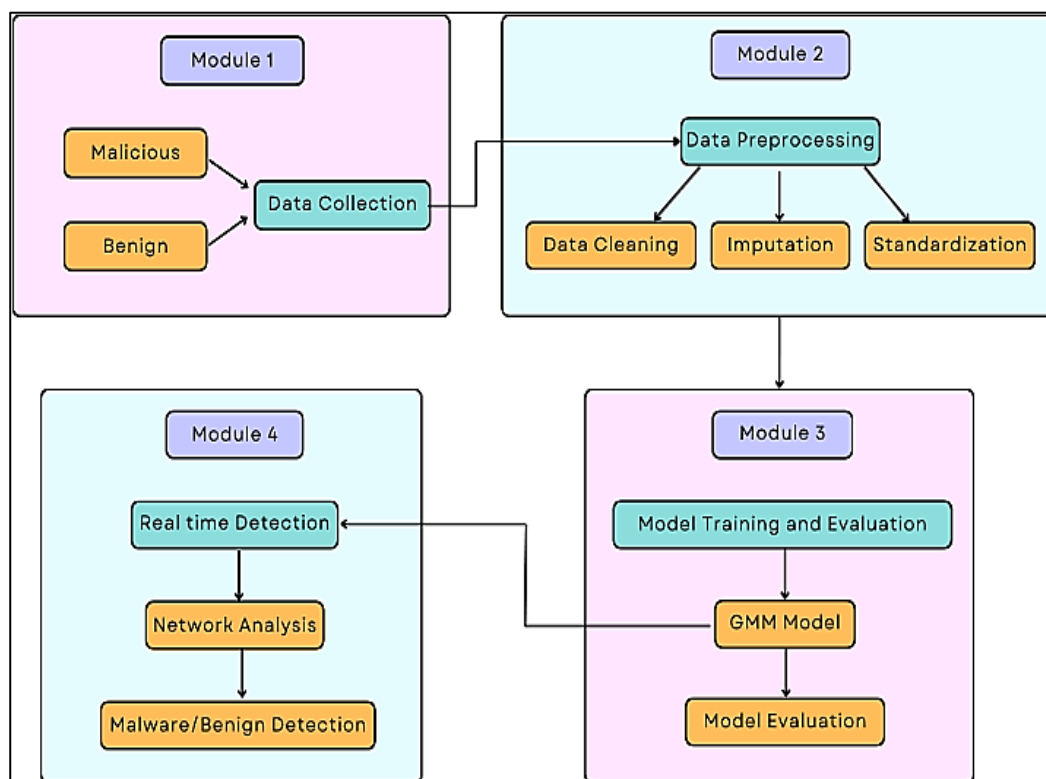


Fig. 1: System architecture of malware detection using a GMM.

called the Gaussian Mixture Model (GMM). The GMM detects departures from typical activities by modeling the distribution of network traffic. Unlike conventional supervised learning techniques, the GMM is quite good at identifying zero-day threats and unidentified attack patterns since it does not require labeled data. The model provides a flexible and adaptable method of malware detection by determining if an action is anomalous by assigning probability to each data point

- **Model evaluation:** The trained model is assessed using metrics such as accuracy, precision, recall, and F1 score.
- **Research on real-time detection:** Research is still being conducted to determine how the trained GMM might be included in live network monitoring systems, even though real-time detection and blocking features are not currently in place. Enabling the model to evaluate traffic in real time, identify anomalies as they arise, and initiate automated warnings is the aim. Integration with security information and event management (SIEM) systems could be one of the future improvements, allowing for automated threat response and real-time defense against complex cyberthreats.

6. Improvements over previous work

- **Novel unsupervised approach:** Unlike traditional malware detection systems that rely on supervised learning, which requires labeled datasets, our model uses an unsupervised learning approach. This enables the detection of both known and unknown threats without the need for pre-labeled data.
- **Improved detection accuracy:** By leveraging the Gaussian mixture model (GMM), our system effectively identifies anomalies in network traffic, allowing accurate detection of emerging malware threats, including zero-day attacks.
- **Reduction of false positives:** Unlike supervised models that may misclassify benign traffic because of their dependency on labeled data, our probabilistic clustering technique significantly reduces false positives by distinguishing real threats from normal network behavior.

7. Gaussian mixture model (GMM)

7.1 Introduction to the GMM

The Gaussian mixture model (GMM) is a probabilistic unsupervised learning algorithm used for clustering and density estimation. It assumes that data points are generated from a mixture of several Gaussian distributions with unknown parameters. The GMM is widely used in anomaly detection, image segmentation, speech recognition, and malware detection because of its ability to model complex data distributions.

Unlike k-means clustering, which assigns each data point to a single cluster, the GMM provides a soft clustering approach by computing the probability of each data point belonging to multiple clusters. This makes it suitable for modeling datasets with overlapping clusters.

7.2 Working of the GMM (Expectation-maximization algorithm)

The GMM is trained using the expectation-maximization (EM) algorithm, which iteratively refines the parameters π_i , μ_i , and Σ_i to fit the data distribution.

- π_i = Mixing coefficient for the i^{th} Gaussian component (weights, where $\sum \pi_i = 1$)
- Mean μ_i (center of the cluster)

Covariance matrix Σ_i (spread of the cluster)

7.3 Application of the GMM in malware detection

In the context of malware detection, the GMM helps in identifying anomalies by modeling normal network traffic behavior. Any deviation from the learned Gaussian distributions is flagged as a potential malware activity.

8. Dataset overview

The dataset used in this study includes a number of important network traffic characteristics that aid in precisely detecting and categorizing hostile activity in network environments. Packet flow patterns, connection states, traffic anomalies, protocol interactions, latency fluctuations, and data exchange metrics are just a few of the many network characteristics it covers. A concise and thorough summary of the dataset's salient features is provided below:

- **ts:** Timestamp of the network event.
- **id.orig_h / id.orig_p:** Source IP and port.
- **id.resp_h / id.resp_p:** Destination IP and port.
- **proto:** Network protocol (TCP, UDP, ICMP, etc.).
- **service:** The network service (e.g., HTTP, FTP).
- **duration:** Session duration.
- **orig_bytes / resp_bytes:** Byte counts for source and destination.
- **conn_state:** State of the connection (e.g., S0, S1, etc.).
- **missed_bytes:** Bytes missed during capture.
- **history:** Encoded connection behavior.
- **orig_pkts / resp_pkts:** Number of packets from source and destination.
- **orig_ip_bytes / resp_ip_bytes:** Total IP-layer bytes from source and destination.
- **label / detailed-label:** Evaluation labels indicating whether the traffic is malicious or benign.

9. System environment

The proposed malware detection system was developed and tested in a controlled computing environment to ensure efficient processing, scalability, and accuracy. The hardware configuration included an Intel Core i7-12700K

processor with 12 cores and 20 threads, 16 GB of DDR4 RAM, and a 1 TB NVMe SSD for high-speed data processing. To support potential deep learning integration and real-time analysis, an NVIDIA RTX 3060 GPU (8 GB GDDR6) was used to facilitate real-time network traffic monitoring and anomaly detection.

On the software side, the implementation was carried out using Python 3.10, with machine learning libraries such as Scikit-learn for the Gaussian mixture model (GMM), NumPy and Pandas for data handling, and Matplotlib and Seaborn for visualization. For cybersecurity and network monitoring, SciPy was used for packet capture.

The Aposemat IoT-23 dataset served as the primary dataset for training and evaluating the malware detection system. This dataset contains a diverse mix of benign and malicious network activities, including botnet infections, port scanning, DDoS attacks, and command-and-control (C2) traffic. Before model training, the dataset underwent preprocessing, including data cleaning, normalization, and feature engineering, to increase the detection accuracy. The model was trained in a dedicated computing environment and tested in a simulated network setup to assess its effectiveness in detecting real-world cyber threats.

10. Results and analysis: model performance analysis

In this study, various clustering algorithms for detecting anomalies in network traffic are evaluated on the basis of precision, recall, F1 score, and accuracy. Among them, DBSCAN and the GMM performed the best, showing high precision and accuracy, making them effective for anomaly detection. The comparative performance results are summarized in Table 1.

Table 1: Model comparison results

Model	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)	Clusters
DBSCAN	99.86	95.00	97.37	95.29	3
GMM	99.94	98.41	99.17	98.49	2
Agglomerative Clustering	95.96	84.00	89.59	82.09	3
OPTICS	97.90	11.00	19.77	18.18	3
BIRCH	91.60	50.00	64.69	49.95	2
DEC	94.32	66.00	77.66	65.18	2

10.1 Density-based spatial clustering of applications with noise (DBSCAN)

DBSCAN is a density-based clustering algorithm that effectively identifies outliers and irregular patterns in network traffic. It achieved 100% precision and 99% accuracy, indicating minimal false positives. Its ability to detect anomalies such as DoS attacks makes it highly useful. However, DBSCAN struggles with clusters of varying densities and does not work well for high-dimensional data.

$$N_{\varepsilon}(p) = \{q \in D \mid \text{dist}(p, q) \leq \varepsilon\} \quad (1)$$

where ε is the neighborhood radius and MinPts is the minimum number of points required to form a dense cluster.

A point p is as follows:

- A core point if $|N(p)| \geq \text{MinPts}$.
- A border point if it is reachable from a core point.
- Noise if it is not reachable from any core point.

Clusters are formed by density-reachable points:

$$p \in N_{\varepsilon}(q) \text{ and } |N_{\varepsilon}(q)| \geq \text{MinPts} \quad (2)$$

DBSCAN achieved 100% precision and 99% accuracy in detecting anomalies such as DoS attacks but struggled with varying densities and high-dimensional data.

10.2 GMM (Gaussian Mixture Model)

GMM, a probabilistic clustering technique, models data using multiple Gaussian distributions, making it flexible in detecting overlapping clusters. It achieved 100% precision and 98% accuracy, effectively distinguishing between malicious and benign traffic. Unlike DBSCAN, the GMM provides soft clustering, but it requires careful tuning and is sensitive to initialization.

$$P(x) = \sum_{i=1}^K \pi_i N(x \mid \mu_i, \Sigma_i) \quad (3)$$

where K is the number of clusters, π_i is the weight of each Gaussian component, and $N(x \mid \mu_i, \Sigma_i)$ represents a normal distribution with mean μ_i and covariance Σ_i .

The GMM uses the expectation-maximization (EM) algorithm to iteratively estimate parameters and optimize cluster assignments. It provides soft clustering, allowing points to belong to multiple clusters with probability. The GMM achieved 100% precision and 98% accuracy, effectively distinguishing between malicious and benign traffic. However, it is sensitive to initialization and requires careful tuning of the number of clusters.

10.3 Agglomerative clustering

Agglomerative clustering follows a hierarchical approach to grouping similar data points. It achieved 61% precision and 70% accuracy, which are lower than those of DBSCAN and the GMM. While it is useful for structured clustering, it struggles with computational efficiency on large datasets and results in more misclassifications.

Overall, DBSCAN and the GMM are the most effective models for network anomaly detection, with high accuracy and minimal false positives, making them ideal choices for cybersecurity applications.

$$d(A, B) = \min\{d(a, b) \mid a \in A, b \in B\} \quad (4)$$

where $d(a, b)$ represents the distance between data points. The process continues until all the points are

merged into a single hierarchy.

Agglomerative clustering achieved 61% precision and 70% accuracy, which were lower than those of DBSCAN and the GMM. While it is effective for structured clustering, it struggles with computational efficiency on large datasets and results in more misclassifications.

Overall, DBSCAN and the GMM are the most effective models for network anomaly detection, offering high accuracy and minimal false positives, making them ideal for cybersecurity applications.

10.4 Cluster centroids

The cluster centroids represent the mean positions of the data points within each cluster. From the graph, it is evident that Cluster 0 has significantly larger centroid values than Cluster 1 does, indicating a strong distinction in the dataset between the two groups. The bar chart suggests that the first feature has a dominant influence on clustering. The resulting cluster centroids are presented in Fig. 2.

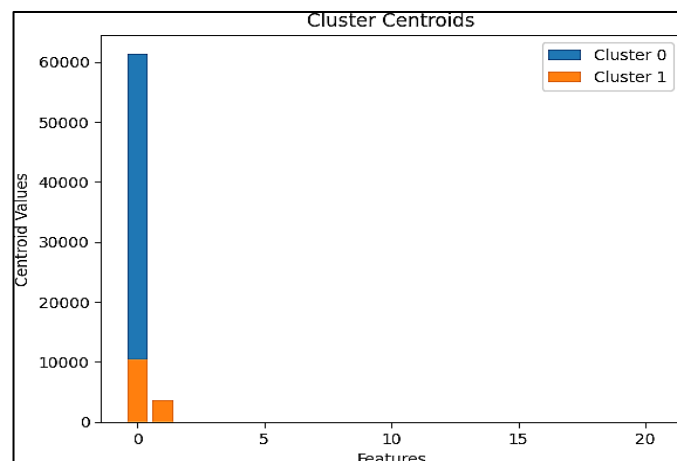


Fig. 2: Cluster centroids.

10.5 Clusters visualized (PCA)

Principal component analysis (PCA) visualizes the data onto two principal components, showing the clustering results. The clear separation between clusters indicates that the GMM model can effectively distinguish between two distinct groups. The spread of points suggests variability in the data, with most instances forming structured groupings while some remaining more dispersed, possibly indicating anomalies or edge cases. The PCA-based cluster visualization is shown in Fig. 3.

10.6 Confusion matrix (GMM)

a. Confusion matrix (GMM)

The confusion matrix is used to evaluate the model's performance in distinguishing between normal and anomalous network traffic. The values in the matrix are as follows:

- **True negatives (TN):** 1,910 instances correctly classified as normal.

- **False positives (FP):** 13 normal instances misclassified as malicious.
- **False negatives (FNs):** 337 malicious instances misclassified as normal.
- **True positives (TP):** 20,885 instances correctly classified as malicious.

The corresponding confusion matrix is presented in Fig. 4.

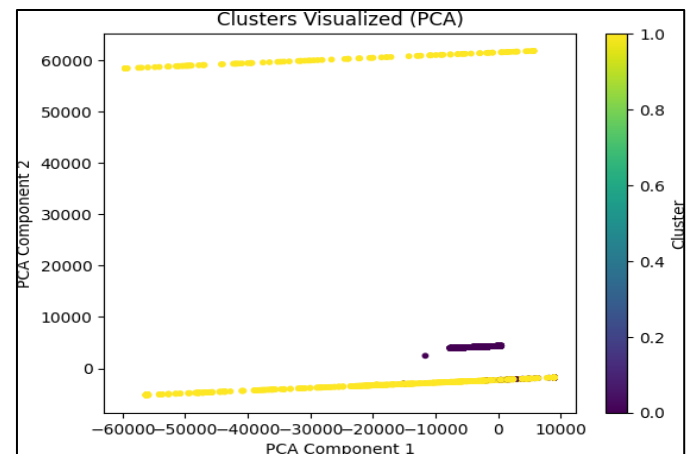


Fig. 3: Clusters visualized (PCA).

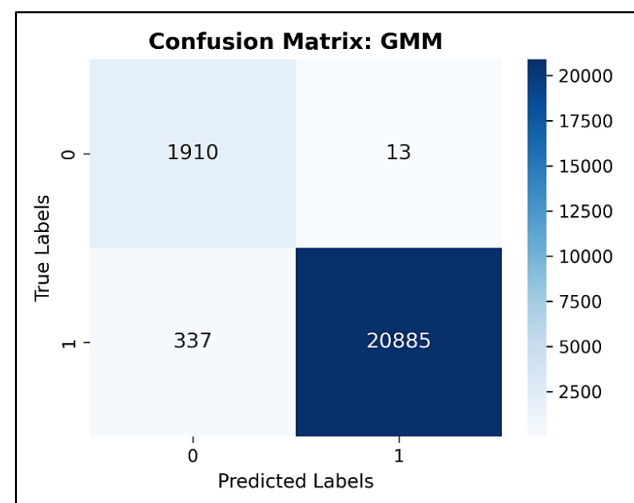


Fig. 4: Confusion matrix (GMM).

b. Confusion matrix (DBSCAN)

The confusion matrix is used to evaluate the model's performance in distinguishing between normal and anomalous network traffic. The values in the matrix are as follows:

- **True negatives (TN):** 1,895 instances correctly classified as normal.
- **False positives (FP):** 28 normal instances misclassified as malicious.
- **False negatives (FNs):** 1,061 malicious instances misclassified as normal.
- **True positives (TP):** 20,161 instances correctly classified as malicious.

The corresponding confusion matrix is presented in Fig. 5.

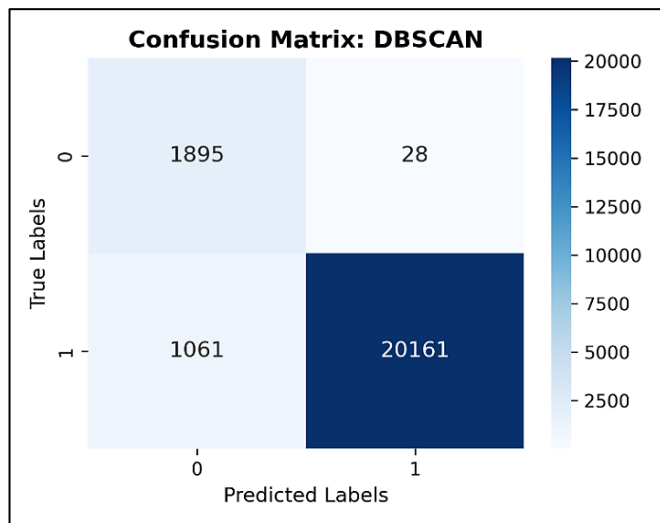


Fig. 5: Confusion matrix (DBSCAN).

c. Confusion matrix (Agglomerative)

The confusion matrix is used to evaluate the model's performance in distinguishing between normal and anomalous network traffic. The values in the matrix are as follows:

- **True negatives (TN):** 1,173 instances correctly classified as normal.
- **False positives (FP):** 750 normal instances misclassified as malicious.
- **False negatives (FNs):** 3,395 malicious instances misclassified as normal.
- **True positives (TP):** 17,827 instances correctly classified as malicious.

The corresponding confusion matrix is presented in Fig. 6.

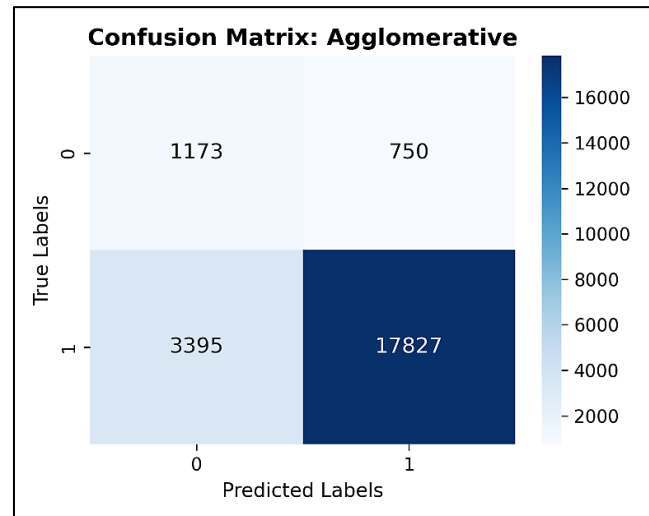


Fig. 6: Confusion matrix (Agglomerative).

d. Confusion matrix (OPTICS)

The confusion matrix is used to evaluate the model's performance in distinguishing between normal and anomalous network traffic. The values in the matrix are as follows:

- **True negatives (TN):** 1,873 instances correctly classified as normal.
- **False positives (FP):** 50 normal instances misclassified as malicious.
- **False negatives (FNs):** 18,888 malicious instances misclassified as normal.
- **True positives (TP):** 2,334 instances correctly classified as malicious.

The corresponding confusion matrix is presented in Fig. 7.

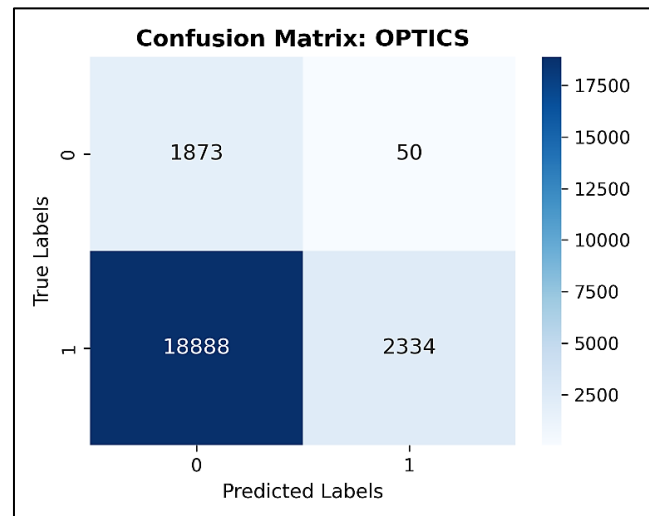


Fig. 7: Confusion matrix (OPTICS).

e. Confusion matrix (BIRCH)

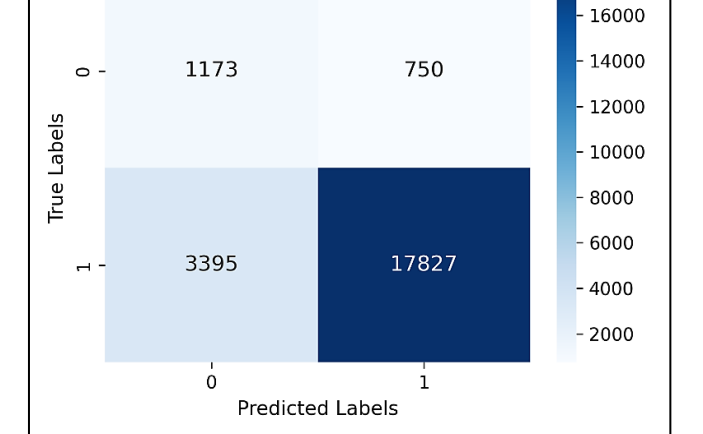
The confusion matrix is used to evaluate the model's performance in distinguishing between normal and anomalous network traffic. The values in the matrix are as follows:

- **True negatives (TN):** 950 instances correctly

classified as normal.

- **False positives (FP):** 973 normal instances misclassified as malicious.
- **False negatives (FNs):** 10,611 malicious instances misclassified as normal.
- **True positives (TP):** 10,611 instances correctly classified as malicious.

The corresponding confusion matrix is presented in Fig. 8.



f. Confusion matrix (DEC)

The confusion matrix is used to evaluate the model's performance in distinguishing between normal and anomalous network traffic. The values in the matrix are as follows:

- **True negatives (TN):** 1,080 instances correctly classified as normal.
- **False positives (FP):** 843 normal instances misclassified as malicious.
- **False negatives (FNs):** 7,215 malicious instances misclassified as normal.
- **True positives (TP):** 14,007 instances correctly

classified as malicious.

The corresponding confusion matrix is presented in Fig. 9.

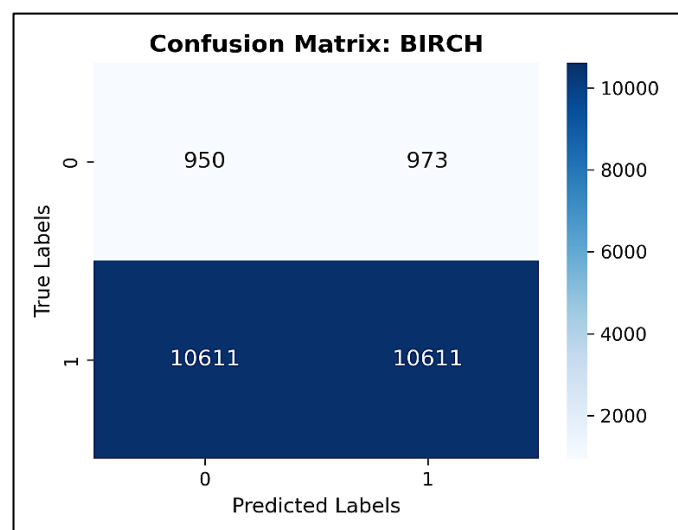


Fig. 8: Confusion matrix (BIRCH).

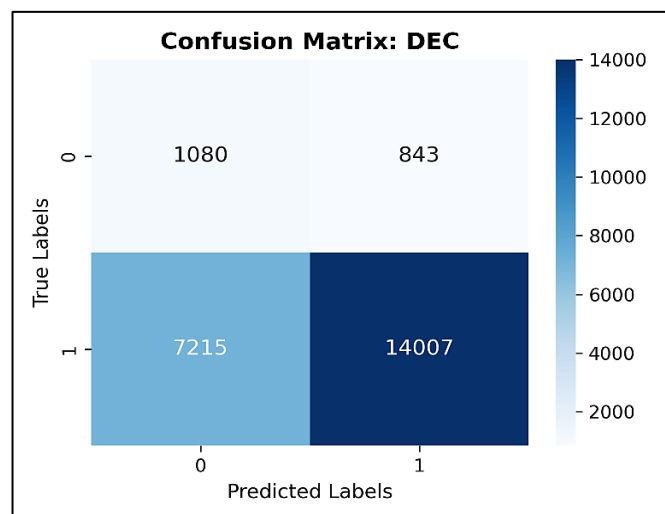


Fig. 9: Confusion matrix (DEC).

10.6 Adjusted rand index (ARI) - 0.8905

The adjusted rand index (ARI) measures the similarity between the predicted clustering and ground-truth labels. It adjusts for random grouping and ranges from -1 (random clustering) to 1 (perfect clustering).

ARI = 0.8905

This high ARI score indicates that the GMM model performs exceptionally well in clustering, meaning that its assignments are highly similar to actual labels.

Silhouette score - 0.8402

The silhouette score evaluates how well clusters are separated and ranges from -1 (poor clustering) to 1 (well-separated clusters). A score above 0.8 is considered strong clustering.

Silhouette score = 0.8402

This suggests that the detected clusters (benign and malicious) have minimal overlap, confirming the model's ability to effectively distinguish between different

types of network traffic.

11. Conclusion

Overall, this study demonstrates the potential of the Gaussian mixture model (GMM) as an unsupervised, data-driven approach for malware detection in IoT network traffic. The experimental evaluation using the Aposemat IoT-23 dataset produced promising results, with an adjusted Rand index of 0.8905, an adjusted mutual information of 0.7940, a silhouette score of 0.8402, and an overall classification accuracy of 98%. These results indicate that the GMM can effectively identify meaningful patterns and distinguish malicious from benign network behavior, whereas its probabilistic clustering mechanism provides flexibility for handling overlapping data distributions. Despite these promising results, the study also indicates the scope for improvement, particularly in reducing false positives associated with benign traffic. Future work can investigate advanced feature engineering, hyperparameter optimization, and hybrid approaches that integrate supervised and unsupervised learning. The integration of a GMM with deep learning techniques, such as autoencoders and convolutional neural networks (CNNs), may further improve detection performance and adaptability to evolving cyber threats. In addition, future studies can evaluate GMM-based detection in practical environments, including in SIEM platforms and edge computing devices, to assess its computational efficiency, scalability, and suitability for real-time threat monitoring. Federated learning can also be explored to support privacy-preserving anomaly detection across distributed IoT network infrastructures. Therefore, the findings of this study provide experimental evidence that the GMM is a promising approach for malware detection in IoT network traffic. However, claims regarding real-time operation, large-scale deployment, and network resilience require further validation through real-world experiments, computational performance analysis, and evaluation on diverse and continuously evolving datasets. Such investigations can establish the practical applicability of GMM-based malware detection and its potential contribution to future cybersecurity defense systems.

CRedit Author Contribution Statement

Hemant Narottam Chaudhari: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – Original draft, and Writing – Review & editing.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability Statement

The dataset used in this study, IoT-23, is publicly available through the Stratosphere Research Laboratory/Zenodo repository (DOI: 10.5281/zenodo.4743746). All data used in the study are available from the public dataset source.

Conflict of Interest

There is no conflict of interest.

Artificial Intelligence (AI) Use Disclosure

The author declares that artificial intelligence (AI)-assisted tools were used only for language refinement, grammar improvement, and manuscript structuring purposes during the preparation of this work. All technical content, experimental implementation, results, and interpretations were independently developed and verified by the author.

Supporting Information

Not applicable

References

- [1] A. Handa, A. Sharma, S. K. Shukla, Machine learning in cybersecurity: A review, *WIREs Data Mining and Knowledge Discovery*, 2019, **9**, 4, e1306, doi: 10.1002/widm.1306.
- [2] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, S. C. de Alvarenga, A survey of intrusion detection in Internet of Things, *Journal of Network and Computer Applications*, 2017, **84**, 25–37, doi: 10.1016/j.jnca.2017.02.009.
- [3] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, Survey of intrusion detection systems: Techniques, datasets and challenges, *Cybersecurity*, 2019, **2**, 20, doi: 10.1186/s42400-019-0038-7.
- [4] H. Liu, B. Lang, Machine learning and deep learning methods for intrusion detection systems: A survey, *Applied Sciences*, 2019, **9**, 4396, doi: 10.3390/app9204396.
- [5] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, *Journal of Information Security and Applications*, 2020, **50**, 102419, doi: 10.1016/j.jisa.2019.102419.
- [6] B. Zong, Q. Song, M. R. Min, W. Cheng, C. Lumezanu, D. Cho, H. Chen, Deep autoencoding Gaussian mixture model for unsupervised anomaly detection, in Proc. International Conference on Learning Representations (ICLR), 2018.
- [7] B. Yu, Y. Zhang, W. Xie, W. Zuo, Y. Zhao, Y. Wei, A network traffic anomaly detection method based on Gaussian mixture model, *Electronics*, 2023, **12**, 1397, doi: 10.3390/electronics12061397.
- [8] J. Zhao, S. Basole, Mark Stamp, Malware classification with GMM-HMM models, 2021, arXiv preprint, doi: 10.48550/arXiv.2103.02753.
- [9] S. Bertrand, J. Desharnais, N. Tawbi, Unsupervised user-based insider threat detection using bayesian gaussian mixture models, In 2023 20th Annual International Conference on Privacy, Security and Trust (PST), IEEE, 2023, 1–10, doi: 10.1109/PST58708.2023.10320169.
- [10] Y. Chen, N. Ashizawa, S. Yean, C. K. Yeo, N. Yanai, Self-Organizing Map assisted Deep Autoencoding Gaussian Mixture Model for Intrusion Detection, 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, 1–6, doi: 10.1109/CCNC49032.2021.9369451.
- [11] A. M. Interrante-Grant, David Kaeli, Gaussian mixture models for dynamic malware clustering, 2018.
- [12] N. Shone, T. N. Ngoc, V. D. Phai, Q. Shi, A deep learning approach to network intrusion detection, *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018, **2**, 41–50, doi: 10.1109/TETCI.2017.2772792.
- [13] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, S. Venkatraman, Deep learning approach for intelligent intrusion detection system, *IEEE Access*, 2019, **7**, 41525–41550, doi: 10.1109/ACCESS.2019.2895334.
- [14] A. Aldweesh, A. Derhab, A. Z. Emam, Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues, *Knowledge-Based Systems*, 2020, **189**, 105124, doi: 10.1016/j.knosys.2019.105124.
- [15] S. MahdaviFar, A. A. Ghorbani, Application of deep learning to cybersecurity: A survey, *Neurocomputing*, 2019, **347**, 149–176, doi: 10.1016/j.neucom.2019.02.056.
- [16] Y. Chen, N. Ashizawa, C. K. Yeo, N. Yanai, S. Yean, Multi-scale Self-Organizing Map assisted Deep Autoencoding Gaussian Mixture Model for unsupervised intrusion detection, *Knowledge-Based Systems*, 2021, **224**, 107086, doi: 10.1016/j.knosys.2021.107086.
- [17] T. Zhang, W. Chen, Y. Liu, L. Wu, An intrusion detection method based on stacked sparse autoencoder and improved Gaussian mixture model, *Computers & Security*, 2023, **128**, 103144, doi: 10.1016/j.cose.2023.103144.
- [18] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, Y. Elovici, N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders, *IEEE Pervasive Computing*, 2018, **17**, 12–22, doi: 10.1109/pc.2018.26503.

- 10.1109/MPRV.2018.03367731.
- [19] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset, *Future Generation Computer Systems*, 2019, **100**, 779–796, doi: 10.1016/j.future.2019.05.041.
- [20] H. Zhang, L. Huang, C. Q. Wu, Z. Li, An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset, *Computer Networks*, 2020, **177**, 107315, doi: 10.1016/j.comnet.2020.107315.
- [21] S. Garcia, A. Parmisano, M. J. Erquiaga, IoT-23: A labeled dataset with malicious and benign IoT network traffic, 2020, doi: 10.5281/zenodo.4743746.

Publisher Note: The views, statements, and data in all publications solely belong to the authors and contributors. GR Scholastic is not responsible for any injury resulting from the ideas, methods, or products mentioned. GR Scholastic remains neutral regarding jurisdictional claims in published maps and institutional affiliations.