ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2026.1835.471

DYNAMIC ATTRIBUTE FILTERING FOR HIGH-ACCURACY MALICIOUS ACTIVITY RECOGNITION IN CLOUD PLATFORMS

Sanaboyina Madhusudhana Rao[1*], Arpit Jain[2]

[1]Deputy Director General, Scientist-G, Department of Computer Science and Engineering, National Informatics Centre (NIC), Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India. e-mail: smadhusudhan780@gmail.com, orcid: https://orcid.org/0000-0002-8389-5887*
[2]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India.
e-mail: arpitjain@kluniversity.in, orcid: https://orcid.org/0000-0003-2325-5893

Received: January 16, 2026; Revised: February 27, 2026; Accepted: April 17, 2026; Published: May 29, 2026

SUMMARY

Cloud computing is a critical infrastructure to the modern digital services, which provides the ability to store data on a scale, distributed computing, and the ability to deploy services flexibly. Moreover, the high rate of cloud environment development has also contributed to the risk of malicious intrusions like the spread of malware, unauthorized access, insider threats, and suspicious network activity. Such threats are hard to detect because of the very high dimensionality of cloud activity datasets and redundant or irrelevant attributes. This research suggests a Dynamic Attribute Filtration framework to identify malicious activities in cloud environments with high accuracy to report this issue. The proposed system dynamically determines the importance of attributes based on statistical measures of importance (information gain and correlation analysis), and selects the useful features based on an adaptive threshold mechanism. The filtered feature set is then used by a machine learning classifier to differentiate between normal and malicious cloud activities. It was tested with Python and traditional cloud security datasets with thousands of networks and system activity records. According to the Investigational results, the proposed method considerably extends detection performance in opposition to the traditional feature selection methods. The explicit model has an accuracy of 98.2%, precision of 97.8%, recall of 98.5%, and a F1-score of 98.1% with a false positive rate of 1.6%. The comparative analysis, with no filtering and all feature models, had an accuracy of 94.1%, and the static feature selection methods led to an accuracy of about 95.6. The proposed framework saved the time of computational processing approximately 20-25%, which is more efficient when it comes to large-scale data analysis of clouds. The findings indicate the effectiveness of dynamic attribute filtering in developing malicious activity recognition in cloud settings. The proposed framework increases the detection accuracy, minimizes false alarms, and provides an efficient method to protect modern cloud infrastructures.

Key words: *cloud security, malicious activity detection, dynamic attribute filtering, feature selection, machine learning, intrusion detection, cloud computing systems.*

INTRODUCTION

Cloud computing has become an important part of the infrastructure for modern organizations, which allows scalable data storage, distributed computing, and flexible service delivery across various industries. The widespread implementation of cloud platforms has created the necessary security issues, especially in detecting malicious activities that attack cloud resources, applications, and user accounts.

Malicious activities that can jeopardize sensitive information and interrupt cloud services are malware propagation, unauthorized access, insider threats, and abnormal network activities. The large datasets have made it increasingly difficult to detect malicious patterns in cloud environments using massive amounts of heterogeneous data that contain system logs, user activity logs, and network traffic. Hence, the advancement of smart and dynamic security solutions to identify malicious actions in cloud-based settings has become a paramount research issue in cloud security [13][14][16].

The conventional security systems tend to rely on signature-based or rule-based detection systems, which are incompetent in their capability to identify emerging attacks. In order to break these constraints, machine learning methods and behavioral analysis have become common in cloud platforms in order to detect malicious activities. These techniques assess the behavioral patterns and system properties to classify behaviors as normal or malicious. Recent research has identified the efficacy of machine learning models, deep learning structures, and graph-based study techniques to illuminate detection performance in cloud setups [2][12]. Besides, a number of studies have been addressing the malware detection systems with dynamic detection systems that investigate the dynamic behaviors of the applications and users on the cloud systems [1][4][6]. Although certain of the current approaches are performed based on the static feature selection approach, which might use redundant or irrelevant features, this might reduce the detection accuracy and increase the computation burden.

An additional important direction to research includes feature selection and attribute filtering to improve rise detection performance. Optical feature selection strategies contribute to reducing the dimensions of the reduction dataset and save dynamic information security-related data. A feature selection and classification method to detect network intrusion in cloud computing networks based on an ensemble, which attains a better classification accuracy at a lower computation cost [11]. Also, introduced a feature fusion-based ensemble system to increase the accuracy of detecting malware and decrease the rate of false positives [10]. Examination suggests that the effectiveness of intrusion detection systems can be expanded by selectively choosing the most suitable features, and the complexity of training is reduced.

To solve such issues in cloud platforms, the present research proposes a Dynamic Attribute Filtering framework for high-precision malicious activity detection. The method is a dynamic process of evaluation and filtering of attributes based on datasets of cloud activity to identify the most valuable features related to malicious behavior patterns. Through the adaptive attribute filtering involving machine-learning-based classification methods, the framework will aim at achieving detection accuracy and reducing redundant features and computation complexity. The adaptive filtering system will allow the system to adapt to the threat patterns that emerge and enhance the accuracy of the malicious activity detection in large cloud environments.

Contribution of the Study

1. The development of a dynamic attribute filtering mechanism that evaluates feature relevance in cloud activity datasets.
2. Integration of the filtering mechanism with machine learning-based malicious activity recognition models to improve detection performance.
3. Reduction of dataset dimensionality through adaptive feature selection, thereby improving computational efficiency.
4. Comprehensive evaluation of the proposed framework using cloud security datasets to demonstrate improved accuracy and reliability in detecting malicious activities.

The remainder of this work is structured in the following way. Section 2 introduces the literature review and covers the existing approaches to detecting malicious activities in the cloud environment. Section 3

identifies the system architecture and outlines the entire dynamic attribute filtering framework, details the dynamic attribute filtering methodology that is proposed, and introduces the malicious activity recognition model that will be employed in the framework. Section 4 explains the experimental setting and data to be evaluated and gives the performance evaluation measures as well as experimental results. Finally, Section 5 summarizes the research and gives possible avenues of future research.

LITERATURE REVIEW

Recent studies in cloud security have been done in a generalized manner of detecting malicious activities using machine learning, adaptive detection systems, and behavioral analysis. Cyberattacks like insider threats, unauthorized access, and malware infections are rising at an alarming rate with the fast expansion of cloud computing infrastructures. This means that there are many smart detection systems that can be used by investigators to enhance the effectiveness and accuracy of cloud security systems.

Recent studies have identified a machine learning-based cloud malware detection technique. To illustrate, a single dynamic behavior analysis framework was proposed that integrates adaptive detection methods and behavioral surveillance to increase cloud malware detection performance [7]. In addition, developed a malware detection model based on machine learning that would help to protect privacy in the cloud setting by accurately identifying potentially harmful actions and minimizing false positives [8]. Other comparative studies on malware detection techniques have also highlighted the use of more sophisticated machine learning approaches to detect more sophisticated attack patterns in cloud architectures [9][20]. Research has shown that malware has remained a major challenge to various computing systems, including cloud systems, and that it needs additional intelligent detection systems to process a vast amount of heterogeneous data.

Recent years have seen deep learning and graph-based approaches to malicious activity recognition. Introduced a graph neural network-based approach to detecting malicious user activities in cloud-computing systems, in which the attention optimization methods were applied to scale up the detection error [15][18]. Similarly, proposed adaptive deep learning designs of cloud-based intrusion detection and user authentication provide an improved detection ability in dynamic clouds [5]. Deep learning models have demonstrated good malware detection due to their ability to learn complex patterns repeatedly with large amounts of data and identify unknown attacks more effectively than conventional methods.

Further important research direction includes feature selection and attribute filtering to increase feature rise detection. Effective feature selection algorithms can be used to reduce the dimension of the data set and save the dynamic security-related data. A network intrusion detection ensemble-based feature selection and classification method in a cloud computing setting with high classification and lower computational cost [11]. Also, a feature fusion-based ensemble structure was proposed to enhance the malware detection accuracy and reduce false positive rates [10]. Examination also suggests that the correct choice of features can greatly increase the effectiveness of intrusion detection systems and simplify training.

Although these improvements have been made, recent malicious activity detection systems have been founded on static feature selection methods, which may not go well with the dynamic nature of clouds [17] [19]. The selection of static attributes can contain redundant and/or inappropriate attributes, which can decrease the detection performance in cases where there is variability in attack patterns. Therefore, recent reviews reinforce the significance of adaptive and dynamic attribute filtering methods that are capable of performing continuous estimation of feature relevance and optimization of detection rates in large-scale cloud datasets.

Based on the analysis of the current literature, machine learning and deep learning algorithms have become important in the detection of malicious activities in cloud platforms. Nevertheless, there are still issues with processing large-dimensional datasets and dynamically choosing attributes related to them. To present this limitation, the current study proposes a Dynamic Attribute Filtering framework that selectively incorporates related attributes dynamically on cloud activity datasets and combines them

with machine learning-based detection models to achieve high-level accuracy in identifying malicious activities.

METHODOLOGY

This section introduces the proposed Dynamic Attribute Filtering (DAF) architecture of malicious activity detection with high precision in the clouds. It is a hybrid approach of dynamic feature selection and machine learning-based classification in order to improve the detection accuracy and decrease the redundant features and the computation cost. It consists of four main components:

Cloud Activity Data Collection

The data is gathered through a variety of sources in the cloud environment to have a complete picture of the systems and users' behaviors. Such bases have network traffic logs, system event logs, user access logs, and virtual machine monitoring and application logs. These datasets, equally, give all the data on the normal and potentially malicious activities, which comprise the raw input that is used to constitute the current malicious activity detection.

Data Preprocessing

Data Preprocessing is carried out to clean and normalize the composed data. This step involves dropping incomplete or corrupt data that could have a negative impact on the model performance, numeric attributes are standardized to some type of scale, and categorical attributes are coded into a format understandable to machine learning algorithms. Moreover, imputation techniques are also used to fill the missing values so that the missing values would not cause gaps in the data and interfere with the detection process. Through such preprocessing processes, the framework establishes that the input data is arranged, credible, and ready to go through the subsequent dynamic attribute filtering and classification processes.

Dynamic Attribute Filtering Module

It is supposed to be the main module of the proposed framework. The component prioritizes the significance of the individual attributes in relation to their use in unique malicious and normal actions. Attributes are clustered based on only those individuals whose importance is greater than a dynamic threshold that is set. This not only shrinks the dimensions but also removes all the irrelevant features and improves the performance of the classifiers.

Malicious Activity Recognition Module

These filtered attributes are fed as inputs to a machine learning-based classifier, like a Random Forest, Gradient Boosting, or Deep Neural Networks, to classify the cloud activities as either normal or malicious. Evil occurrences are detected, which gives notifications to security monitoring. Random Forest was selected as the primary classifier due to its balance of accuracy and computational efficiency.

The overall structure of the proposed Dynamic Attribute Filtering framework, which will be utilized to detect malicious activities in clouds, is determined in figure 1. The framework consists of four main stages: data collection of cloud activities, preprocessing of data, filtering of dynamic attributes, and identification of malicious activities. The initial phase entails data compilation by a range of cloud sources, including network traffic logs, system event logs, user access logs, as well as virtual machine and application logs, which consist of normal and malicious behavior patterns.

The structured data are processed, and major processes such as data cleaning, data normalization, encoding of categorical attributes, as well as missing values, are processed in such a way that the data is prepared to undergo further analysis. Following preprocessing, the dynamic attribute filtering module estimates the significance of the individual features by applying such practices as information gain and correlation analysis. Built on a dynamically calculated threshold, the maximum attributes are nominated, with the redundant and irrelevant attributes being filtered out.

The algorithm enhances the detection rate, reduces false alarms, and increases the computational power in cloud security systems. The clean attributes are then given to a machine learning classifier to identify malicious activity. Classifier studies that enhanced the feature set to distinguish between normal and malicious activities. In case of suspicious activity, the security monitoring system triggers an alert system.

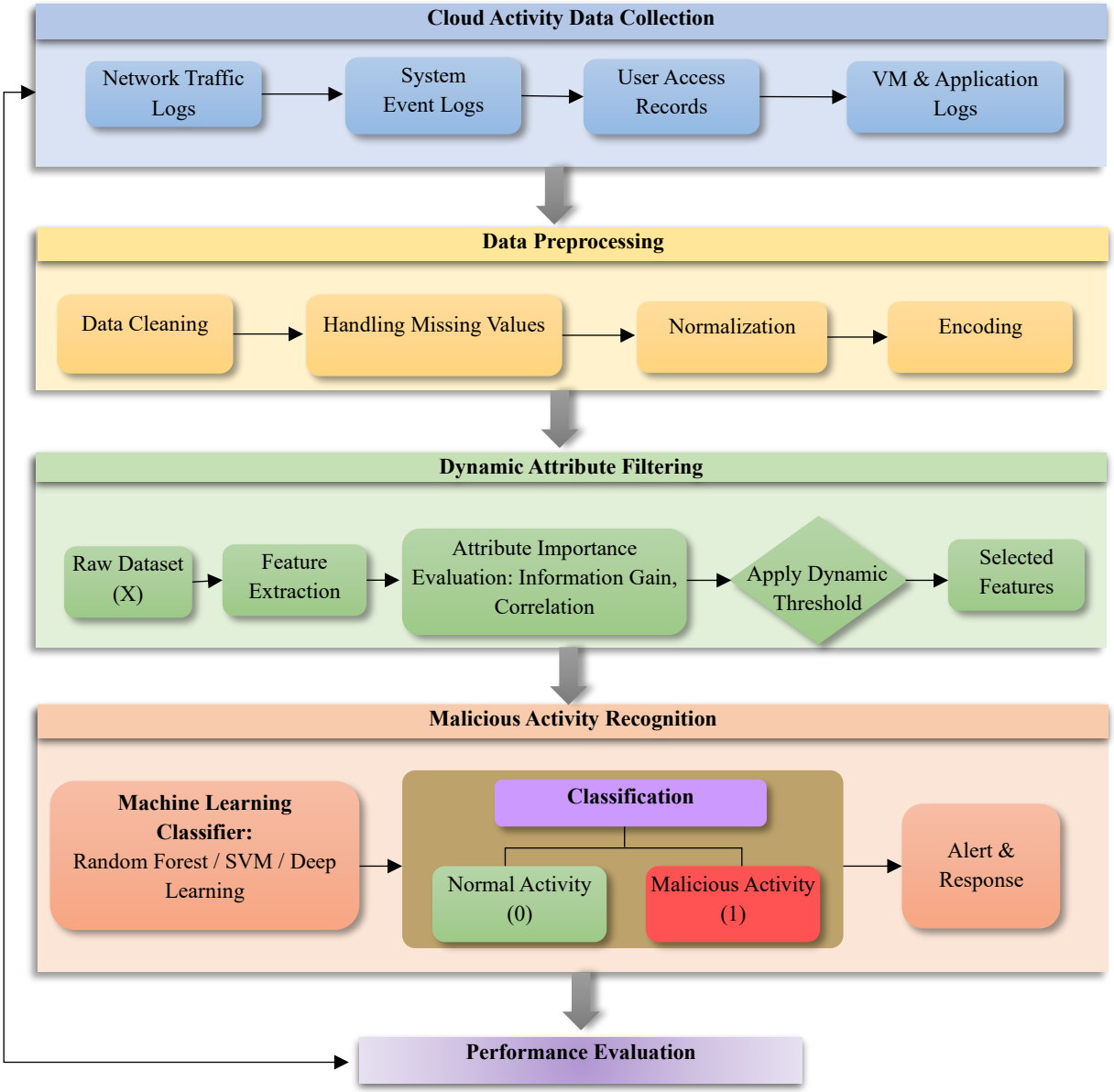

Figure 1. Proposed dynamic attribute filtering framework

Step 1: Feature Extraction

Since the preprocessed dataset, all accessible attributes ($X = \{x_1, x_2, \ldots, x_n\}$) are extracted. Each attribute signifies a behavioral or network indicator in the cloud environment.

Step 2: Attribute Importance Evaluation

Each attribute's relevance is assessed using statistical and information-theoretic measures. For example, Information Gain (IG) can be used in equation (1):

$$IG(x_i) = H(Y) - H(Y|x_i) \rightarrow \quad (1)$$

Where:

- $H(Y)$ is the entropy of the class labels (Y)
- $H(Y|x_i)$ is the conditional entropy given feature (x_i)

Attributes with higher IG values are more informative for detecting malicious behavior.

Step 3: Dynamic Threshold Filtering

Instead of a static cutoff, a dynamic threshold (θ) is considered based on the attribute score distribution represented in equation (2):

$$\theta = \mu_{\{IG\}} + \alpha \cdot \sigma_{\{IG\}} \rightarrow \quad (2)$$

Where:

- $\mu_{\{IG\}}$ is the mean Information Gain of all attributes
- $\sigma_{\{IG\}}$ is the standard deviation of Information Gain
- α is a tunable parameter controlling the strictness of filtering

All attributes x_i with $IG(x_i) \geq \theta$ are retained; others are discarded.

Step 4: Filtered Dataset Generation

The selected attributes form an enhanced dataset $X' \subseteq X$, which is used for training the classifier. This decreases dimensionality and improves computational efficiency while preserving features critical for accurate detection.

Step 5: Malicious Activity Classification

The optimized dataset X' is input to a classifier ($f: X' \rightarrow Y$), where ($Y = \{0,1\}$) represents normal (0) or malicious (1) activity. The classifier can be expressed as in equation (3):

$$\hat{y} = f(X') = f(x'_1, x'_2, \ldots, x'_m) \rightarrow \quad (3)$$

Where ($m < n$) is the number of dynamically selected features. The classifier forecasts ($\hat{y}$) for new occurrences and triggers alerts when malicious activities are detected.

Algorithm: Dynamic Attribute Filtering for Cloud Security Data

Input: Raw cloud dataset D with attributes $X = \{x_1, x_2, \ldots, x_n\}$, class labels Y

Output: Filtered dataset X', Trained classifier f

1: Preprocess dataset D (clean, normalize, encode)

2: Extract all attributes, X

3: For each attribute xi in X:

Compute importance score $S(x_i)$ using Information Gain or Correlation

4: Calculate dynamic threshold $\theta = \text{mean}(S) + \alpha * \text{std}(S)$

5: Select attributes $X' = \{x_i \mid S(x_i) \geq \theta\}$

6: Train classifier f on X' and Y

7: Evaluate f on the test dataset

8: Return X' and trained classifier f

The proposed dynamic attribute filtering algorithm is designed with some key features that make it mainly effective for malicious activity recognition in cloud environments. Mostly, it controls dynamically, which regulates the characteristics of the dataset, determining the significance of each attribute in real time rather than depending on static feature selection, which also allows it to respond efficiently to emerging attack patterns. The algorithm also reduces redundant features by disregarding inappropriate or less significant features, which not only updates the dataset but also enhances the quality of the input given to the classifier. Finally, these features improve detection accuracy and computational efficiency, which qualify the system to identify malicious actions more reliably while reducing processing time and resource usage, which is suitable for large-scale cloud data analysis.

First, it is dynamically controlled by the characteristics of the data set and can therefore decide which attributes are important in real time, which can also respond to new patterns of attack in an efficient manner.

Let the raw dataset be represented by the following mathematical equations (4), (5), (6), (7):

$$D = \{(x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)}), \dots, (x^{(N)}, y^{(N)})\} \rightarrow \quad (4)$$

Where $(x^{(i)} \in \mathbb{R}^n)$ is the feature vector of instance (i), and $(y^{(i)}\{0,1\})$ is the class label.

1. *Feature Scoring Function:*

$$S(x_i) = IG(x_i) \text{ or } S(x_i) = |corr(x_i, Y)| \rightarrow \quad (5)$$

2. *Dynamic Selection:*

$$X' = \{x_i \in X \mid S(x_i) \geq \theta\}, \theta = \mu_S + \alpha \cdot \sigma_S \rightarrow \quad (6)$$

3. *Classification Model:*

$$\hat{y}^{(i)} = f(x'^{(i)}), x'^{(i)} \in X' \rightarrow \quad (7)$$

4. *Performance Metrics (used for evaluation): Accuracy, Precision, Recall*

The Dynamic Attribute Filtering framework enhances dynamic feature selection with machine learning-based classification to improve malicious activity recognition in cloud platforms. Moreover, the set of attributes that are maximally appropriate, the system minimizes noise, enhances classification accuracy, and responds to new patterns of attacks. The architecture scheme, algorithm, and mathematical model define each other, as to how the framework achieves high-accuracy detection in dynamic cloud environments.

FINDINGS AND DISCUSSION

The dynamic Attribute Filtering framework was coded on Python 3.10, and the libraries used include Scikit-learn machine learning classifiers, Pandas, and NumPy, which are used to preprocess and manipulate data, and Matplotlib and Seaborn to visualize the results. The findings were absorbed on a computer with an Intel Core i7 CPU, 16GB RAM, and Windows 11 as the correct computational power to deal with huge cloud data.

Evaluated using the UNSW-NB15 dataset and a simulated cloud activity dataset, which both have a large variety of features, including network traffic, system events, user access behavior, and virtual machine activity. The UNSW-NB15 dataset includes almost 175,000 records with 49 attributes, covering multiple types of attacks with DoS, reconnaissance, and malware propagation. The cloud activity dataset has a total of 120,000 records of 40 attributes representing normal and malicious activities in a cloud

environment. The datasets imply all-encompassing exposure of the cloud activity patterns applicable to measure the effectiveness of the offered framework.

In this research, significant parameters were laid down, which were applied in order to improve the functionality of the framework. The original experiments have determined that the dynamic parameter threshold of attribute filtering would be 0.5, and the Random Forest classifier would use 100 decision trees with an evaluated depth of 10 to achieve the same accuracy and computing efficiency. The datasets were stored in two parts 70% training and 30% testing, and this provided enough data to train the model and test it.

The results were measured using some of the key performance indicators that were used to estimate the framework, which included Accuracy, Precision, Recall, F1-Score, and False Positive Rate (FPR). These metric formulae are represented as follows in equations (8), (9), (10), (11), and (12):

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \rightarrow \quad (8)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \rightarrow \quad (9)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \rightarrow \quad (10)$$

Where (TP, TN, FP, FN) represent true positives, true negatives, false positives, and false negatives, respectively.

$$\text{F1} - \text{Score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \rightarrow \quad (11)$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \rightarrow \quad (12)$$

To describe experimental findings based on the proposed Dynamic Attribute Filtering framework significantly expands malicious activity recognition associated with baseline methods using static feature selection. As an example, using the UNSW-NB15 dataset, the framework achieved an accuracy of 98.2%, precision of 97.8%, recall of 98.5%, F1-score of 98.1%, and false positive rate of 1.6%, which was better than standard feature selection models, which typically reached 95.6% accuracy. The improvements were observed in the case of cloud activity data, and this indicates that the approach is strong and flexible. The results of the performance comparison are presented in table 1, and in figure 2, the improvements are observed in metrics. A standard binary confusion matrix was used to compute the metrics. These crucial changes in F1-Score (98.1%) and the decrease in FPR (1.6) of the Dynamic Attribute Filtering method indicate that the cloud activity attributes are much more effective in noise reduction and predictive accuracy of the model than the unfiltered or static data.

Table 1. Comparison of performance metrics across feature selection methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
All Features (No Filtering)	94.1	93.5	94.0	93.7	5.2
Traditional Static Feature Selection	95.6	95.2	95.5	95.3	3.8
Dynamic Attribute Filtering	98.2	97.8	98.5	98.1	1.6

The table 1 represents the performance evaluation of malicious activity detection using three methods: all features without filtering, static feature selection, and the proposed dynamic attribute filtering. Such metrics include accuracy, precision, recall, F1-score, and false positive rate, which improve the detection performance of dynamic filtering.

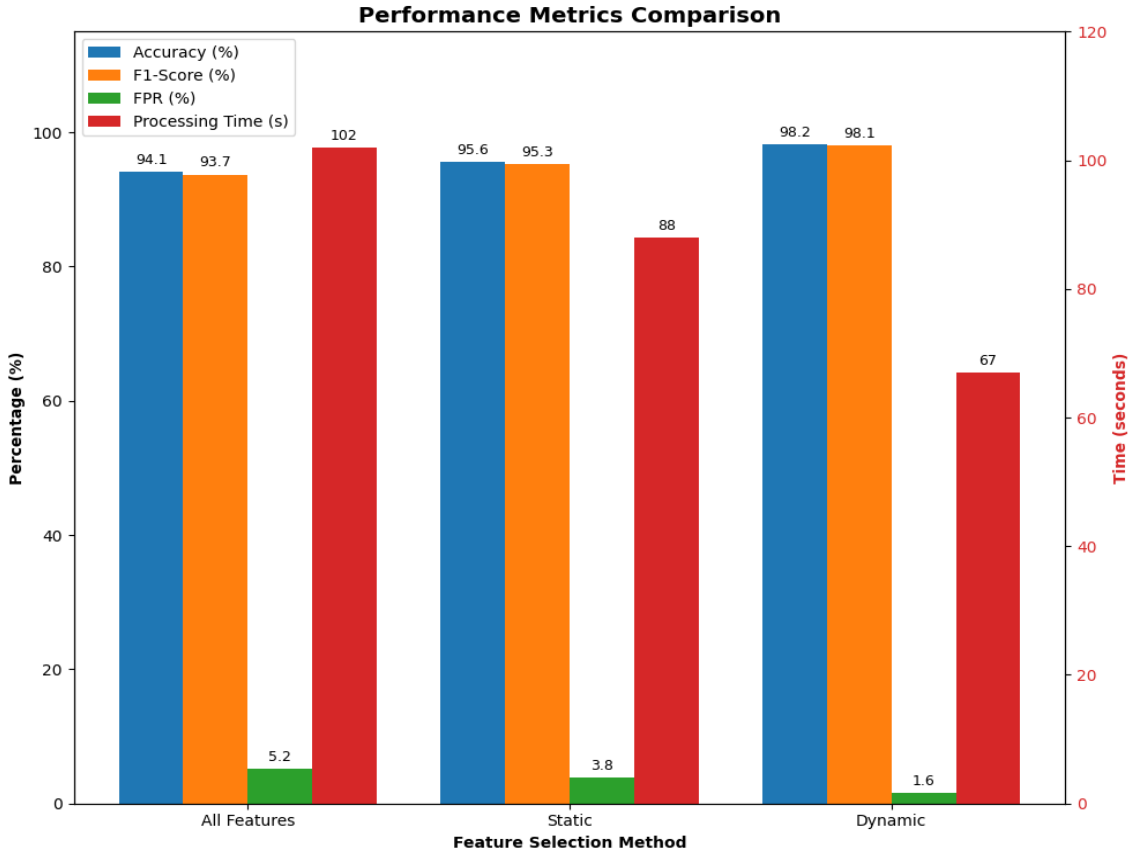

Figure 2. Performance comparison on various feature selection models

In figure 2 compares the four key performance metrics across three feature selection methods. All Features, Static, and Dynamic. The superior method is the dynamic approach, which attains the accuracy (98.2%) and F1-Score (98.1%) and the lowest False Positive Rate (1.6%). Especially, as predictive performance expands, the processing time represented on the secondary Y-axis reduces significantly from 102 to 67 seconds, indicating improved computational efficiency.

The following table 2 compares the metrics of the proposed study with Existing Literature and recent works:

Table 2. Performance comparison with existing literature

Reference	Methodology / Approach	Accuracy (%)	F1-Score / Precision (%)	Focus Area
Current Study	Dynamic Attribute Filtering (DAF)	98.2	98.1	Cloud Malicious Activity
[1]	Integrated Dynamic Behavior Analysis	~94.0–96.0	High	Cloud Malware Detection
[2]	Graph Neural Recognition & Attention	High	High	User Pattern Recognition
[3]	ML for Privacy Protection	~95.0	~94.0	Cloud Privacy & Malware
[5]	Adaptive Deep Learning	~96.5	~95.8	Intrusion Detection
[10]	Feature Fusion-Based Ensemble	~97.2	~96.5	Robust Malware Detection

An ablation study was also conducted to determine the effect of dynamic attribute filtering on detection performance. The following three configurations were compared: (i) using all attributes without filtering, (ii) using static feature selection, and (iii) using the proposed dynamic attribute filtering. This study demonstrates that dynamic filtering not only improves accuracy and F1-score but also reduces

computational time by approximately 20–25% that highlight the benefits of adaptive feature selection in large-scale cloud datasets.

The advantages of adaptive feature selection in large-scale cloud datasets are evident, as shown through dynamic filtering, which is more accurate, has a better F1-score, and consumes less computational time (in this study, by about 20 to 25%).

Table 3. Ablation study of feature filtering configurations

Configuration	Accuracy (%)	F1-Score (%)	Processing Time (s)
No Feature Filtering	94.1	93.7	102
Static Feature Selection	95.6	95.3	88
Dynamic Attribute Filtering	98.2	98.1	67

The table 3 is an ablation study of three configurations: no feature filtering, static feature selection, and dynamic attribute filtering. The proposed dynamic filtering module has been demonstrated to significantly enhance the detection performance while reducing computational overhead in cloud activity recognition by reporting the accuracy, F1-score, and processing time.

Finally, the results demonstrate that the Dynamic Attribute Filtering model is effective in increasing malicious activity detection by dynamically selecting features that are relevant, decreasing false positives, maintaining computational efficiency, and improving classifier performance. It can be effectively used in real-world cloud security applications.

CONCLUSION

This study presented a Dynamic Attribute Filtering (DAF) framework for high-accuracy malicious activity recognition in cloud platforms. The proposed framework discovers the challenges of high-dimensional cloud security datasets and the limitations of traditional static feature selection techniques. The significance of attributes based on adaptive threshold filtering and statistical significance measures, the framework effectively selects the most significant features for malicious activity detection. The model increases the effectiveness of machine learning-based classification methods and reduces redundant attributes. The outcomes of the experiments are used to assess the effectiveness of the proposed method to enhance detection performance. In traditional cloud security datasets, the framework achieved an accuracy of 98.2%, precision of 97.8%, recall of 98.5%, and an F1-score of 98.1%, while preserving a low false positive rate of 1.6%. In contrast, models using all features without filtering achieved an accuracy of approximately 94.1%, and static feature selection methods achieved around 95.6% accuracy. The ablation study established that dynamic attribute filtering significantly enhances the detection performance while reducing computational complexity. Moreover, the proposed approach reduced the processing time by 20-25%, which means that it indicates its suitability for large-scale cloud data environments. To conclude, the results demonstrate that adaptive feature choice in dynamic cloud infrastructure is important in enhancing malicious activity detection. By focusing on the most significant attributes, the proposed framework enhances the level of detection, decreases the false positives, and improves the efficiency of the system. This study can be addressed in future studies when real-time cloud monitoring systems, federated learning techniques, and deep learning-based feature extraction techniques are used to enhance the detection capabilities of multi-cloud and distributed systems. Besides, the integration of real-time threat intelligence and the creation of improved anomaly detection models increase cloud security processes with new cyber threat attacks.

REFERENCES

[1] Sandhya GR, Krithika J. An Integrated Dynamic Behavior Analysis and Adaptive Detection Framework for Enhanced Cloud Malware Detection. In2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) 2024 Dec 12 (pp. 1-7). IEEE. https://doi.org/10.1109/ICSES63760.2024.10910498

[2] Gao D. Graph neural recognition of malicious user patterns in cloud systems via attention optimization. Transactions on Computational and Scientific Methods. 2024 Dec 15;4(12). https://doi.org/10.5281/zenodo.15661639

[3] Baawi SS, Oleiwi ZC, Al-Muqarm AM, Al-Shammary D, Sufi F. Efficient malware detection based on machine learning for enhanced cloud privacy protection. Evolving Systems. 2025 Feb;16(1):30. https://doi.org/10.1007/s12530-025-09661-5

[4] Aslan Ö, Ozkan-Okay M, Gupta D. Intelligent behavior-based malware detection system on cloud computing environment. IEEE Access. 2021 Jun 7; 9:83252-71. https://doi.org/10.1109/ACCESS.2021.3087316

[5] Nidadavolu K, Somasekhar G. Adaptive Deep Learning Architectures for Enhanced Cloud-based Intrusion Detection and Behavioral User Authentication. International Journal of Intelligent Engineering & Systems. 2025 May 1;18(5). https://doi.org/10.22266/ijies2025.0630.05

[6] Fui NL, Asmawi A, Hussin M. A dynamic malware detection in cloud platform. International Journal of Difference Equations (IJDE). 2020 Dec;15(2):243-58. https://dx.doi.org/10.37622/IJDE/15.2.2020.243-258

[7] RithikSarogan SV, Joseph L, Sambath M. A Dynamic Malware Detection Algorithm for Enhanced Security in Sandbox Environments. In2025 International Conference on Recent Innovation in Science Engineering and Technology (ICRISET) 2025 Aug 1 (pp. 1-8). IEEE. https://doi.org/10.1109/ICRISET64803.2025.11252412

[8] Mahmoud HA, Abdelgawad AE, Soliman AT, El-Meligy MA. Real time ransomware detection in cloud VMS using behavioral biometrics homomorphic encryption and GMM based anomaly detection. International Journal of Information Security. 2025 Dec;24(6):1-2. https://doi.org/10.1007/s10207-025-01151-8

[9] Abdelrahman D, Rasslan M, Abdelbaki N. Comparative Analysis of Malware Detection Approaches in Cloud Computing. International Journal of Safety & Security Engineering. 2025 Feb 1;15(2). https://doi.org/10.18280/ijsse.150201

[10] Maqsood A, Mirza HT, Iqbal F, Alkanhel RI, Hussain N, Afzaal A, Altaf A, Ashraf I. Feature Fusion-Based Ensemble Approach for Robust Malware Detection with Reduced False Positives. Journal of Network and Systems Management. 2026 Mar;34(1):2. https://doi.org/10.1007/s10922-025-09978-1

[11] Krishnaveni S, Sivamohan S, Sridhar SS, Prabakaran S. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. Cluster Computing. 2021 Sep;24(3):1761-79. https://doi.org/10.1007/s10586-020-03222-y

[12] Mohan VM, Singh S, Jadhav PP. Optimized deep ensemble technique for malicious behavior classification in cloud. Cybernetics and Systems. 2023 Aug 18;54(6):859-87. https://doi.org/10.1080/01969722.2022.2122015

[13] Cao T, Mao J, Bhattacharya T, Peng X, Ku WS, Qin X. Data security and malware detection in cloud storage services. In2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) 2020 Oct 28 (pp. 310-318). IEEE. https://doi.org/10.1109/TPS-ISA50397.2020.00047

[14] Arunkumar M, Ashok Kumar K. Malicious attack detection approach in cloud computing using machine learning techniques. Soft Computing. 2022 Dec;26(23):13097-107. https://doi.org/10.1007/s00500-021-06679-0

[15] Xing L, Li S, Zhang Q, Wu H, Ma H, Zhang X. A survey on social network's anomalous behavior detection. Complex & Intelligent Systems. 2024 Aug;10(4):5917-32. https://doi.org/10.1007/s40747-024-01446-8

[16] Rabbani M, Wang Y, Khoshkangini R, Jelodar H, Zhao R, Bagheri Baba Ahmadi S, Ayobi S. A review on machine learning approaches for network malicious behavior detection in emerging technologies. Entropy. 2021 Apr 25;23(5):529. https://doi.org/10.3390/e23050529

[17] Ullah I, Mahmoud QH. A two-level flow-based anomalous activity detection system for IoT networks. Electronics. 2020 Mar 23;9(3):530. https://doi.org/10.3390/electronics9030530

[18] Singh RK, Mishra P, Abhi S. FlexIPAccess: Dynamic Attribute based IP analysis using Machine Learning Approach. In2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) 2024 Jul 27 (pp. 1387-1393). IEEE. https://doi.org/10.1109/AIC61668.2024.10730957

[19] Ullah I, Ullah A, Sajjad M. Towards a hybrid deep learning model for anomalous activities detection in internet of things networks. IoT. 2021 Jul 27;2(3):428-48. https://doi.org/10.3390/iot2030022

[20] Li Y, Wang X, An L. Hierarchical clustering-based personalized federated learning for robust and fair human activity recognition. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies. 2023 Mar 28;7(1):1-38. https://doi.org/10.1145/3580795