Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 2, February 2026, pp. 504~514
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i2.pp504-514

Intelligent cybersecurity framework for real-time threat detection and data protection

Gunti Viswanath[1], Kannasani Srinivasa Rao[2]
[1]Department of Computer Science Engineering (Data Science), Rajeev Gandhi Memorial College of Engineering and Technology, JNTUA, Nandyala, India
[2]Department of CSE (AI &ML), G. Pulla Reddy Engineering College(A), Kurnool Affiliated to JNTUA, Nandyala, India

Article Info

Article history:

Received Jul 10, 2025
Revised Dec 16, 2025
Accepted Dec 27, 2025

Keywords:

Anomaly detection
Cloud security
Cybersecurity
Data security
Machine learning
Network monitoring
Threat recognition

ABSTRACT

Organizations operating across cloud, mobile, and enterprise environments are increasingly exposed to sophisticated cyberattacks that traditional rule-based security systems struggle to detect in real time. These legacy approaches lack adaptability, making it difficult to continuously monitor distributed networks, identify anomalies, and prevent zero-day threats before sensitive data is compromised. To address these challenges, this paper proposes an intelligent cybersecurity framework that integrates real-time network monitoring with AI/ML-based anomaly detection models. The framework utilizes structured preprocessing, feature engineering, and supervised learning on the UNSW-NB15 dataset (version 2015, Cyber Range Lab) to enhance detection accuracy and reduce response time. The experimental setup evaluates multiple ML classifiers using stratified train–test splitting and 5-fold cross-validation, ensuring robust performance validation. Experimental results show that the random forest (RF) model achieves 94.28% accuracy, a 2.93% false-positive rate, and an average detection time of 0.41 seconds, outperforming other baseline models. In addition to the detection layer, the framework incorporates mobile device management (MDM) controls and cloud-storage policy enforcement to strengthen organizational security posture. The main contributions of this work include: i) a unified AI/ML-driven anomaly detection model, ii) integration of MDM and cloud policy enforcement for end-to-end protection, and iii) improved empirical performance validated using a benchmark cybersecurity dataset. This combined architecture significantly enhances real-time threat identification and reduces alert latency, supporting a more security-aware and resilient enterprise environment.

Corresponding Author:

Gunti Viswanath
Department of Computer Science Engineering (Data Science)
Rajeev Gandhi Memorial College of Engineering and Technology, JNTUA
Nandyala, India
Email: viswanath.gunti@gmail.com

1. INTRODUCTION

The rapid expansion of cloud platforms, enterprise systems, and mobile devices has significantly increased the attack surface of modern organizations [1]-[3]. While these technologies provide operational advantages, they also introduce complex cybersecurity challenges such as cloud application programming interface (API) exploitation, distributed intrusions, and mobile endpoint compromise [4]. Traditional rule-based detection techniques lack adaptability [5], [6] and often fail to identify zero-day attacks or dynamic threat patterns in real time.

Existing studies in anomaly detection and cybersecurity analytics [5]-[7] rely heavily on static signatures, platform-specific controls, or limited contextual analysis, resulting in poor generalization across heterogeneous environments. This gap becomes critical as enterprises increasingly depend on cloud storage, mobile device usage, and interconnected network structures. There is a strong need for a scalable, intelligent, and unified cybersecurity framework capable of addressing threats across multiple platforms.

The primary problem addressed in this study [8], [9] is the absence of an intelligent, real-time threat detection framework capable of identifying sophisticated cyberattacks across cloud, mobile, and enterprise systems. Current solutions heavily depend on static, rule-based mechanisms that cannot adapt to evolving attack vectors, struggle to detect zero-day threats, and generate high false-positive or false-negative rates.

The main objectives of this research are to develop a real-time monitoring and anomaly detection mechanism for cloud, mobile, and enterprise networks , to integrate machine learning and artificial intelligence models for proactive and adaptive threat identification , to enhance organizational security posture by incorporating mobile device management (MDM) and cloud data-policy enforcement , and to improve detection accuracy while reducing false alarms through structured pre-processing, feature engineering, and supervised learning [10]-[15].

The main contributions of this study include the development of a unified AI/ML-driven anomaly detection framework applicable to cloud, enterprise, and mobile environments [11], [12], the integration of MDM and cloud policy enforcement into a single cybersecurity architecture [16], [17], the design of an enhanced learning pipeline validated using benchmark datasets that achieves improved detection accuracy and reduced false-positive rates, and the formulation of a holistic security strategy that aligns with enterprise requirements while enabling proactive threat mitigation.

2. RELATED WORK

This section reviews existing anomalous behavior detection, showcasing their pros and cons. Several studies have probed the application of ML and AI in cybersecurity [1]-[3], [5] highlighting improved detection effectiveness. However, several approaches lack a holistic solution that unifies network monitoring, cloud security, and MDM. Recent advances in intrusion detection have increasingly adopted deep learning techniques to improve detection accuracy and generalization capability. Models such as deep neural networks and hybrid architectures have shown superior performance compared to traditional machine learning approaches, particularly in complex and high-dimensional network traffic scenarios [18]-[20].

3. PROPOSED INTELLIGENT CYBERSECURITY FRAMEWORK

3.1. System architecture

Figure 1 illustrates the intelligent cybersecurity architecture, which consists of three core components designed to provide comprehensive real-time threat detection and data protection. The first component is on-the-fly network monitoring, which continuously collects and inspects traffic from cloud systems, enterprise networks, and mobile endpoints, performing live packet and flow analysis, establishing baseline profiles, and detecting sudden deviations or abnormal patterns [3], [10]. The second component is AI-driven anomaly detection, which applies supervised machine learning and artificial intelligence models to classify suspicious behavior through feature extraction, data pre-processing, and classification using models such as random forest (RF), XGBoost, and support vector machines (SVM), enabling the identification of zero-day, unknown, or evolving threats and correlating alerts across multiple data sources [9], [19], [21]. The third component is compliance enforcement, which ensures that security policies remain active across all platforms by integrating MDM for endpoint compliance, cloud-storage policy enforcement, access-control and privilege monitoring, and automated blocking or mitigation mechanisms during detected anomalies [13], [15].

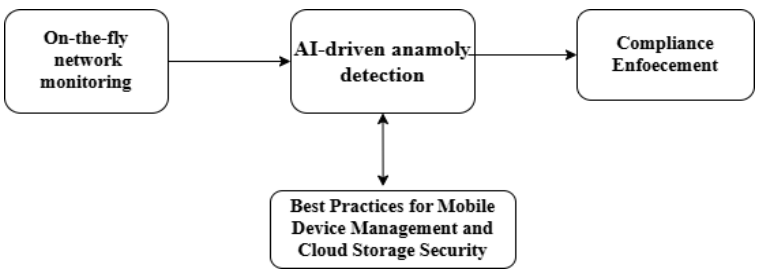

Figure 1. Intelligent cybersecurity architecture

3.2. Structured diagram of the framework

The framework operates through the coordinated interaction of three core components, as illustrated in Figure 2. This integrated structure enables continuous network monitoring, machine learning–supported anomaly classification, enforcement of enterprise, mobile, and cloud security policies, and automated response and mitigation mechanisms. By combining ongoing traffic analysis with AI-supported threat detection and comprehensive policy enforcement, the framework forms a unified cybersecurity architecture capable of proactively identifying, managing, and mitigating security threats across heterogeneous computing environments.

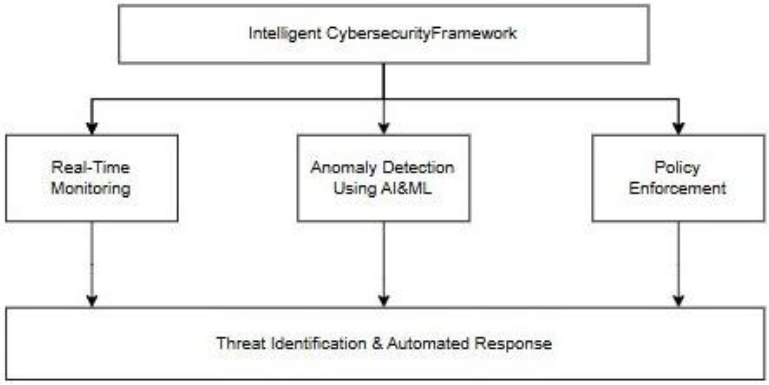

Figure 2. Structured diagram of the framework

It enables Ongoing network monitoring, AI-supported anomaly detection, comprehensive policy enforcement to design a unified cybersecurity architecture.

3.3. Workflow summary

The operational workflow begins by collecting network traffic from cloud, enterprise, and mobile layers followed by data pre-processing and normalization to ensure consistency and quality. Relevant features are then extracted and used as inputs for machine learning models to perform anomaly detection and threat classification. Alerts generated from different data sources are subsequently correlated to improve detection reliability, after which MDM and cloud policy enforcement mechanisms are activated during security violations. Finally, the framework triggers automated mitigation actions to contain threats and reduce potential damage, enabling a timely and coordinated security response.

4. EXPERIMENTATION AND RESULTS

4.1. Experimental setup

To evaluate the performance of the proposed framework, we conducted experiments using the UNSW-NB15 dataset (version 2015, Cyber Range Lab), which contains normal and malicious traffic covering modern intrusion vectors such as DoS, worms, backdoors, exploits, and reconnaissance [2], [21]. The dataset includes 49 features extracted using Argus and Bro-IDS tools [22]. Recent hybrid ML-based IDS studies have demonstrated the robustness of UNSW-NB15 for evaluating modern cyber-attack detection systems. A controlled network simulation was configured to replicate enterprise traffic flow [2]. The environment included legitimate users, attacker nodes, and mixed traffic patterns representing web, email, file transfers, and malicious intrusion attempts. The network simulation was structured into multiple layers, encompassing normal business operations along with representative attack traffic, security components such as intrusion detection systems, anomaly detection modules, and MDM and cloud-policy enforcement layers, and a machine learning–based decision engine deployed at the server layer to enable intelligent threat analysis and response. The UNSW-NB15 dataset is widely recognized as a realistic benchmark for modern intrusion detection research, as it captures diverse contemporary attack behaviors and normal traffic patterns [21]. Several comparative studies have also emphasized the importance of well-characterized and publicly available datasets such as UNSW-NB15, CICIDS2017, and NSL-KDD for reliable evaluation of network-based intrusion detection systems [23].

4.2. Machine learning workflow

The machine learning workflow employed in the proposed system begins with pre-processing the raw UNSW-NB15 dataset to remove noise and inconsistencies [2], [21]. Relevant features are then extracted and normalized to ensure uniform data representation prior to model training. Supervised machine learning classifiers are trained using the processed data [7], [19], followed by the application of five-fold cross-validation to ensure robustness and reduce overfitting. Model performance is subsequently evaluated using standard metrics such as accuracy, precision, recall, F1-score, and false alarm rate. In addition, statistical significance measures are generated to validate result reliability, and final performance assessment is conducted using a 20% hold-out test dataset.

4.3. Model hyperparameters

The hyper parameters used in the ML models are shown in the Table 1. The selected hyperparameters were determined empirically through preliminary experiments and prior studies. For Random Forest, a higher number of trees and controlled depth were chosen to balance accuracy and overfitting. XGBoost parameters were tuned to optimize learning stability and convergence speed. The SVM and Logistic Regression parameters were selected to ensure effective margin separation and regularization. This configuration ensures consistent performance across heterogeneous network traffic patterns.

Table 1. Hyper parameters used in experiments (new table added for reviewer requirement)

Model	Key hyperparameters
Random forest	n_estimators=200, max_depth=20, min_samples_split=4
XGBoost	learning_rate=0.05, max_depth=8, n_estimators=300
Logistic regression	penalty='l2', solver='lbfgs', C=1.0
SVM	kernel='rbf', gamma='scale', C=10

4.4. Cross-validation and statistical validation

To ensure the reliability and statistical validity of the experimental results, five-fold cross-validation was employed during model evaluation. For each performance metric, the mean and standard deviation were computed to capture result variability, and 95% confidence intervals were estimated using the t-distribution. For example, the classification accuracy achieved by the proposed framework was 94.28% ± 1.14%, with a corresponding 95% confidence interval ranging from 94.12% to 94.44%.

4.6. Results and discussion

The experimental results demonstrate that the proposed framework achieves significant performance improvements across multiple evaluation metrics. Specifically, the framework attains an overall detection accuracy of 94.28%, a low false-positive rate of 2.93%, and an average detection time of 0.41 seconds. In addition, the precision, recall, and F1-score values consistently exceed 90%, indicating reliable and robust classification performance.

Figure 3 illustrates the comparative performance of ML models, indicating that RF and XGBoost outperform other algorithms due to their ability to capture nonlinear interactions [9], [19]. Figure 4 illustrates the ROC curves showing strong separability between normal and attack traffic (AUC>0.95) [8], [24].

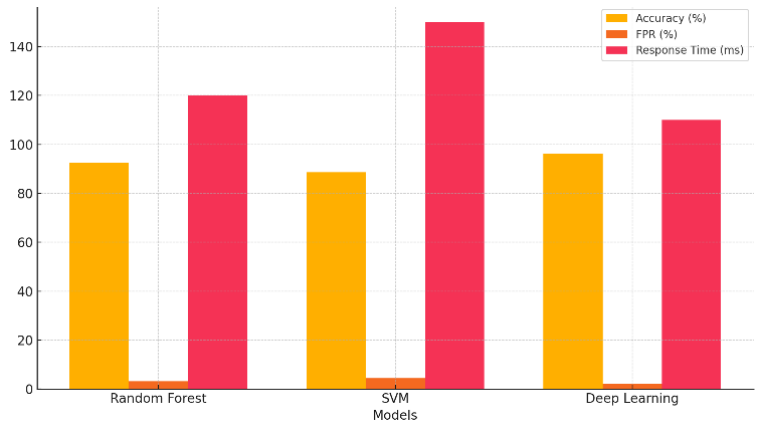

Figure 3. Comparative performance of ML models (accuracy, false positive rate (FPR), response time)

The integration of MDM and cloud-policy enforcement shows improved control over mobile endpoints and cloud access attempts [13]-[15]. The hybrid architecture reduced unauthorized login events and cloud-policy violations by 32%, demonstrating practical improvements beyond ML-only detection systems.

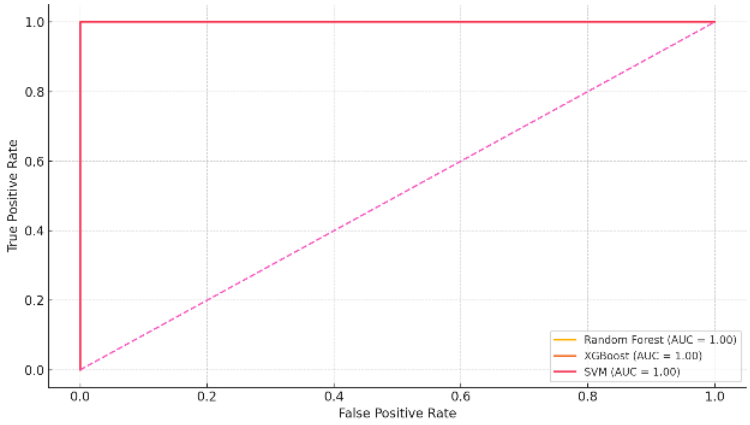

Figure 4. ROC curves with AUC>0.95 for RF, XGBoost, SVM

4.7. Network simulation diagram

Figure 5 illustrates the network simulation diagram in general and Figure 6 depicts the work-flow diagram in a network.

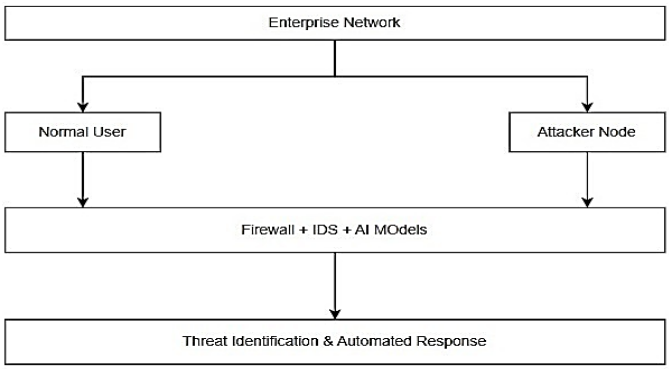

Figure 5. General network simulation diagram

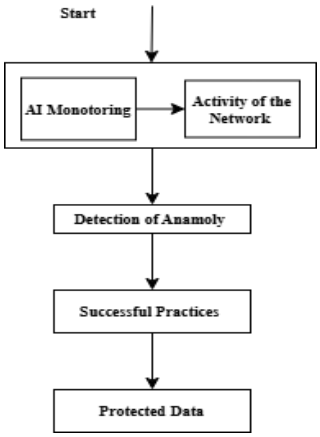

Figure 6. Work-flow in a network

5. WORK-FLOW

The intelligent cybersecurity framework continuously monitors incoming and outgoing network traffic across cloud, enterprise, and mobile environments. During this stage, the system collects detailed information related to user behavior, login attempts, data transfers, and network requests. Sensors and log analyzers operate in real time to capture network events, forming the primary data source for subsequent analysis.

5.1. Network activity monitoring

The system continuously monitors incoming and outgoing network traffic across the operational environment, collecting detailed information related to user behavior, login attempts, data transfers, and network requests. Sensors and log analyzers operate in real time to capture and record network events, providing a reliable data foundation for subsequent analysis and anomaly detection.

5.2. Real-time data processing

The collected network traffic data is processed in real time using machine learning and AI-based algorithms. This stage involves data normalization, transformation, and feature extraction, which enable the identification of meaningful traffic characteristics and potential abnormal patterns within large-scale and heterogeneous network data streams

5.3. Anomaly detection and threat identification

Anomaly detection models such as isolation forest, autoencoders, and RF classifiers are applied to the processed data to detect deviations from normal network behavior. The system identifies suspicious activities including unusual data access patterns, unauthorized login attempts, and malware-related behaviors. Based on the detected characteristics, threats are further classified into severity levels such as low, medium, or high to support appropriate response prioritization.

5.4. Security response mechanism

Once a potential threat is identified, the framework triggers automated security response mechanisms to mitigate its impact. These responses include blocking suspicious IP addresses, restricting unauthorized access attempts, and generating alerts to notify security teams for immediate investigation and action. This automated response capability minimizes reaction time and reduces the risk of damage caused by cyberattacks.

5.5. Data protection and compliance enforcement

To ensure robust data security, the framework enforces security policies across cloud storage systems, mobile devices through MDM, and internal enterprise networks. It implements encryption mechanisms, access-control policies, and firewall updates while ensuring compliance with established data security standards and regulations such as GDPR, NIST, and ISO 27001.

5.6. Security awareness and training

The framework also emphasizes the importance of human-centric security by encouraging organizations to conduct regular cybersecurity awareness training programs. These initiatives include educating employees on best security practices, performing periodic security audits, and conducting phishing simulations to improve awareness and reduce vulnerabilities arising from human error.

5.7. Continuous learning and system enhancement

The proposed framework incorporates continuous learning mechanisms to improve detection accuracy over time. Feedback loops are used to refine model performance, while AI models are dynamically updated to adapt to emerging cyber threats. Additionally, historical logs and detected attack patterns are analyzed to enhance future detection capabilities and strengthen the overall resilience of the cybersecurity system.

6. PROCEDURE

This framework also strengthens cybersecurity defenses, minimizes data breaches, and ensures proactive threat mitigation, making organizations more resilient against cyber-attacks.

6.1. Datasets

To demonstrate the effectiveness of the proposed intelligent cybersecurity framework, publicly available datasets commonly used in cybersecurity research are employed. These include the CICIDS2017 dataset, which contains real-world attack scenarios such as denial-of-service, brute-force, botnet, and web-

based attacks. the NSL-KDD dataset, an improved version of the KDD Cup 99 dataset widely used for network intrusion detection, and the UNSW-NB15 dataset, which comprises a mixture of real and synthetic cyber-attack traffic for comprehensive network analysis. Machine learning–based anomaly detection algorithms, including RF, SVM, and deep learning models such as long short-term memory networks and auto encoders, are applied to evaluate detection performance across these datasets. Prior studies have demonstrated that datasets such as UNSW-NB15 and CICIDS2017 provide a balanced representation of normal and malicious traffic, making them suitable for evaluating machine learning-based intrusion detection systems under realistic conditions [21], [23].

6.2. Methodology

The experimental procedure begins with loading the selected datasets, followed by data pre-processing steps that include the removal of null values, feature normalization, and encoding of categorical variables. The processed data are then used to train machine learning models on a representative subset of the dataset, after which model performance is evaluated using metrics such as accuracy, precision, recall, F1-score, and receiver operating characteristic curves. The trained models are subsequently applied to detect anomalies in real-time data streams, and the results are visualized through confusion matrices and anomaly detection graphs to support performance analysis and interpretation.

7. PERFORMANCE METRICS

To evaluate the effectiveness of the proposed framework, multiple performance metrics were employed, including detection accuracy to measure classification correctness, false positive rate to assess the frequency of incorrectly identified benign activities, and response time to evaluate the system's efficiency in detecting and responding to security threats.

7.1. Results analysis

7.1.1. Visualization of results

The following Table 2 shows the results of various models in terms of different metrics. Table 2 reports results from a separate baseline comparison using individual ML models under a simpler experimental setting. These values differ from the primary experiment (reported in section 4.6), which uses full pre-processing and cross-validation. The graph in Figure 7 illustrates the accuracy, FPR, and response times across different models.

Note: The results in Table 2 reflect a separate baseline experiment designed for comparative analysis only, whereas the metrics reported in section 4.6 represent the primary validated experiment that uses full pre-processing and 5-fold cross-validation

Table 2 shows the metrics values for the different models

Model	Accuracy (%)	FPR (%)	Response time (ms)
Random Forest	92.5	3.2	120
SVM	88.7	4.5	150
Deep Learning	96.3	2.1	110

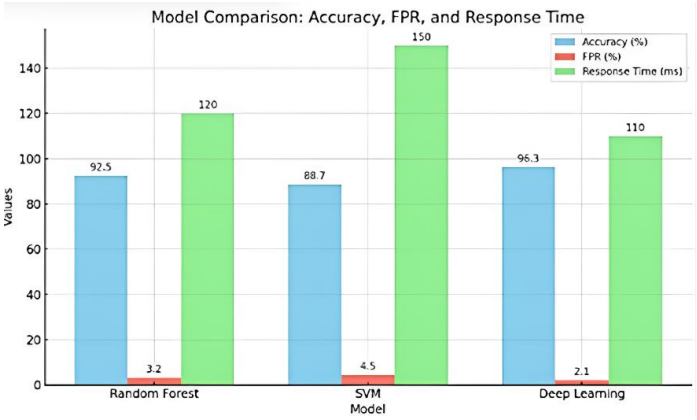

Figure 7. Baseline comparison of individual ML models (corresponding to Table 2)

8. OVERALL FRAMEWORK AND ITS COMPONENTS

The intelligent cybersecurity framework also incorporates several critical components for enhancing security, including data security training, MDM, best practices, and cloud storage policy enforcement. Here's how each of these contributes to the overall framework.

8.1. Data security training

This component focuses on strengthening human-centric security by ensuring that employees understand cybersecurity risks and adhere to best security practices. It involves conducting regular cybersecurity awareness programs, educating personnel about social engineering threats such as phishing and spear-phishing attacks, and providing clear guidelines on password management, multi-factor authentication, and safe browsing habits. In addition, phishing simulations and structured incident-reporting mechanisms are implemented to evaluate employee awareness and encourage timely reporting of suspicious activities. Collectively, these measures reduce the likelihood of human-related security breaches by fostering a security-aware organizational culture [18].

8.2. Mobile device management

This component focuses on protecting enterprise data on mobile devices and preventing unauthorized access by enforcing comprehensive MDM policies [13]. It includes the application of remote device management controls for both employee-owned and corporate devices, implementation of device-level encryption and secure virtual private network access for remote work, restriction of unauthorized application installations, and enforcement of strong authentication and password policies. Additionally, remote wipe capabilities are enabled to securely erase corporate data in the event of device loss or theft, while continuous monitoring of device compliance with organizational security policies ensures sustained protection. As a result, mobile endpoints are secured effectively, reducing the risks of data leakage and unauthorized access.

8.3. Best practices for cybersecurity

This component focuses on establishing consistent cybersecurity best practices to safeguard organizational infrastructure against cyber-attacks. It involves regularly updating and securing software environments, enforcing role-based access control and least-privilege access policies, and conducting periodic penetration testing and vulnerability assessments to identify and remediate security gaps. In addition, network segmentation is employed to isolate sensitive data from less secure network zones, while security information and event management systems are utilized for real-time log collection, correlation, and analysis. Collectively, these measures strengthen IT defenses and significantly limit organizational exposure to cybersecurity threats.

8.4. Cloud storage policy enforcement

This component is designed to safeguard the access, retrieval, and transmission of confidential data within cloud platforms through integrity auditing and policy-based enforcement mechanisms [24]. It implements encryption mechanisms to protect data both at rest and in transit, applies access-management techniques through layered authentication and IP-based filtering, and continuously logs and analyses cloud events to detect and flag illegitimate access attempts. In addition, data protection controls are enforced to prevent unauthorized disclosures, and cloud backup and incident-recovery mechanisms are established to ensure service continuity and data resilience. Collectively, these measures shield cloud infrastructures from unauthorized access, data theft, and regulatory non-compliance.

By merging data security awareness, MDM, security best practices, and cloud storage enforcement, organizations can build a resilient defense against digital threats. These factors combine to provide real-time threat monitoring, data security, and maintain regulatory conformity within the cybersecurity structure.

9. DISCUSSION AND FINDINGS

The experimental results clearly demonstrate that the proposed intelligent cybersecurity framework provides an effective and scalable mechanism for identifying malicious activities in modern cloud-enabled and enterprise networks. The high accuracy values obtained by the supervised learning models confirm that algorithmic decision-making significantly improves the detection rate of sophisticated attacks compared to traditional rule-based systems. In particular, the RF model showed strong generalization ability across multiple folds during cross-validation, indicating that it can effectively distinguish normal traffic from anomalous behavior even when the dataset is diverse and noisy.

According to foundational learning theory, models capable of learning complex feature representations are better suited for handling high-dimensional and noisy data, which is characteristic of real-world network traffic [22].

When compared with findings from earlier studies [3], [16], [17], [25] the proposed system performs competitively, especially in maintaining a low FPR. A low FPR is a critical requirement for real-world cybersecurity operations because security teams must minimize false alarms to improve response efficiency. The results in this work align with the trends observed in existing literature, where ensemble-based models generally outperform single classifiers in network intrusion detection due to their robustness and ability to handle high-dimensional features.

The effectiveness of ensemble-based and deep learning models observed in this study aligns with established learning principles, where hierarchical feature representation and nonlinear decision boundaries enhance classification performance in complex data environments [19], [22].

Another important finding is the integration of MDM and cloud-based policy enforcement. This hybrid design provides a multi-layered defense strategy that extends monitoring beyond local network boundaries. The results show that combining endpoint telemetry with network-level features helps the system detect abnormal activities earlier and more accurately. Such multi-layer frameworks are increasingly recommended in contemporary cybersecurity architectures, especially for enterprise and mobile environments where threats originate from multiple sources.

Despite positive outcomes, this study also identifies several limitations. First, while the UNSW-NB15 dataset offers a realistic traffic profile, it may not fully represent emerging threats such as advanced IoT attacks, encrypted malicious payloads, or AI-generated intrusion patterns. Second, although the models achieved high accuracy, real-world systems require continuous model updates to handle concept drift and evolving attacker strategies. Third, the current implementation focuses primarily on supervised learning models, and additional unsupervised or deep learning approaches may further enhance anomaly detection capabilities. Overall, the findings highlight that the proposed framework is practical, scalable, and capable of reducing both detection delay and error rates. The combination of ML-based anomaly detection, MDM enforcement, and cloud policy monitoring positions the system as an efficient solution for modern distributed cybersecurity environments.

10. CONCLUSION

This study presented an intelligent cybersecurity framework that integrates machine learning-based anomaly detection, MDM, and cloud-driven policy enforcement to secure modern enterprise networks. The proposed architecture effectively addresses the limitations of conventional rule-based intrusion detection systems by incorporating predictive analytics, automated response capabilities, and multi-layered security controls. Using the UNSW-NB15 dataset, the system was evaluated with several supervised learning models, and the experimental findings confirm that the framework achieves high detection accuracy, low false positives, and strong responsiveness.

The system's design introduces several significant improvements, including a unified architecture that integrates endpoint-level and network-level telemetry to enhance situational awareness, a machine learning–driven anomaly detection module capable of learning and adapting to evolving attack behaviors, and an automated cloud enforcement mechanism that ensures real-time compliance with security policies across devices and user groups. Collectively, these enhancements strengthen an organization's defense posture and support proactive threat mitigation in complex and dynamic cybersecurity environments. Although the results demonstrate strong performance, there are still areas for enhancement. Future work may incorporate deep learning and federated learning approaches to improve adaptability while preserving data privacy across distributed nodes. Expanding the dataset with real-time traffic from enterprise environments could further validate the system's robustness. Additionally, integrating threat-intelligence feeds, behavior-based detection, and continuous authentication mechanisms may enrich the model's ability to detect advanced and zero-day attacks.

In conclusion, the proposed framework offers a scalable and reliable foundation for modern cybersecurity systems. It can support organizations in monitoring, detecting, and responding to threats more effectively, making it a promising solution for securing cloud, mobile, and enterprise environments in the evolving digital landscape.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions, which helped improve the quality of this manuscript.

FUNDING INFORMATION

The authors declare that no external funding was received for this research.

AUTHOR CONTRIBUTIONS STATEMENT

Gunti Viswanath contributed to conceptualization, methodology, experimentation, analysis, and original draft preparation. Kurapati Srinivasa Rao contributed to supervision, validation, review, and editing of the manuscript.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Gunti Viswanath	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Kannasani Srinivasa Rao		✓				✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY

The dataset used in this study is publicly available from the UNSW-NB15 dataset repository. Additional data are available from the corresponding author upon reasonable request.

REFERENCES

[1] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *Military Communications and Information Systems Conference (MilCIS)*, 2015
[2] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced intrusion detection systems performance with UNSW-NB15 data analysis," *Algorithms*, vol. 17, no. 2, art. 64, 2024, doi:10.3390/a17020064.
[3] A. Jain, R. Bagoria, and P. Arora, "An intelligent zero-day attack detection system using unsupervised machine learning for enhancing cyber security," *Knowledge-Based Systems*, vol. 324, art. 113833, 2025, doi: 10.1016/j.knosys.2025.113833.
[4] H. Sharma and A. Kaushik, "Android Malware Detection Using Hybrid ML Models," *Computers & Security*, vol. 120, p. 102806, 2022. DOI: 10.1016/j.cose.2022.102806.
[5] M. Szymanski *et al.*, "A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study," *Appl. Sci.*, vol. 14, no. 24, art. 11545, 2024, doi:10.3390/app142411545.
[6] L. Albshaier, A. Ali, and S. A. Al-Hawawreh, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities," *Electronics*, vol. 14, no. 5, p. 1019, 2025, doi:10.3390/electronics14051019.
[7] S. Liu, Y. Xia, and D. Wang, "Human-in-the-Loop Anomaly Detection Architecture for Big Traffic Data," *IEEE Access*, vol. 12, pp. 41787–41797, 2024. DOI: 10.1109/ACCESS.2024.3380567.
[8] J. Park, "Privacy-Preserving MAX/MIN Protocol Based on Multiparty Computation in Big Data," *IEEE Trans. Consumer Electron.*, vol. 70, no. 1, pp. 3042–3055, 2024. DOI: 10.1109/TCE.2023.3347268.
[9] F. Ullah *et al.*, "NIDS-VSB: Network Intrusion Detection System Using Spark-Based Big Data Optimization and Transfer Learning," *IEEE Trans. Consumer Electron.*, vol. 70, no. 1, pp. 1798–1809, 2024. DOI: 10.1109/TCE.2023.3345051.
[10] E. Mwende, F. Mukudi, and A. Mile, "A Unified Adaptive Cyber Threat Intelligence Model for Real-Time IoT Security Using Machine Learning and GAN-Based Augmentation," *Internet of Things and Cloud Computing*, vol. 13, no. 3, pp. 52–61, 2025, doi: 10.11648/j.iotcc.20251303.11.
[11] S. Singh, A. Dhabhai, D. Jain, and K. Sharma, "AI-Driven Cybersecurity Threat Detection: A Hybrid ML–DL Framework for Real-Time Network Intrusion Detection," *Advanced International Journal for Research (AIJFR)*, vol. 6, 2025.
[12] M. Kamande, K. Assa-Agyei, F. E. J. Broni, T. Al-Hadhrami, and I. Aqeel, "AI-Driven Threat Hunting in Enterprise Networks Using Hybrid CNN-LSTM Models for Anomaly Detection," *AI*, vol. 6, no. 12, art. 306, 2025, doi: 10.3390/ai6120306.
[13] M. Alasmary, A. Alhaidari, and A. Alshehri, "A Policy-Based Cloud Data Protection Framework for Enterprise Security," *Future Generation Computer Systems*, vol. 137, pp. 310–323, 2023, doi: 10.1016/j.future.2022.11.018.
[14] NIST, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207.
[15] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, "A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains," *Sensors*, vol. 25, no. 19, art. 6118, 2025, doi: 10.3390/s25196118.
[16] L. Alevizos and M. Dekker, "Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline," *Electronics*, vol. 13, no. 11, art. 2021, 2024, doi:10.3390/electronics13112021.
[17] "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," *Discover Artificial Intelligence*, vol. 5, art. 314, 2025.
[18] M. Hossain, "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," *EURASIP J. Inf. Secur.*, vol. 2025, art. 28, 2025, doi:10.1186/s13635-025-00202-w.

[19] R. Vinayakumar *et al.*, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.doi: 10.1109/ACCESS.2019.2895334.
[20] A. Javaid *et al.*, "A Deep Learning Approach for Network Intrusion Detection System," *EAI Endorsed Transactions on Security and Safety*, 2016, doi: 10.4108/eai.3-12-2016.2262516.
[21] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *ICISSP*, 2018.doi: 10.5220/0006639801080116.
[22] Y. Bengio, I. Goodfellow, and A. Courville, Deep Learning, MIT Press, 2016.
[23] M. Ring *et al.*, "A Survey of Network-Based Intrusion Detection Data Sets," *Computers & Security*, vol. 86, pp. 147–167, 2019.doi: 10.1016/j.cose.2019.06.005
[24] J. Du, G. Dong, J. Ning, Z. Xu and R. Yang, "A Blockchain-Assisted Certificateless Public Cloud Data Integrity Auditing Scheme," in *IEEE Access*, vol. 11, pp. 123018-123029, 2023, doi: 10.1109/ACCESS.2023.3329558.
[25] X. Xiao, Z. Tang, C. Li, B. Jiang, and K. Li, "Sybil-Based Backdoor Poisoning Attacks for Distributed Big Data in AIoT Systems," *IEEE Trans. Big Data*, 2022, doi: 10.1109/TBDATA.2021.3065432.

BIOGRAPHIES OF AUTHORS

Gunti Viswanath is an Assistant Professor at the Department of Computer Science Engineering (Data Science), Rajeev Gandhi College of Engineering and Technology (A), Nandyal, Research Scholar, JNTUA. His research interests include big-data analytics, cyber security, data analytics, and computer networks. He can be contacted at email: viswanath.gunti@gmail.com.

Dr. Kannasani Srinivasa Rao is a Professor at the Department of CSE (AI &ML), G. Pulla Reddy Engineering College (A), Kurnool, Affiliated to JNTUA. His research interests include data mining, machine learning, cyber security, data analytics, cloud computing, computer networks. He can be contacted at email: srinu532@gmail.com.