https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

An Iterative Systematic Analytical Review of Modern Intrusion Detection Systems

Rahul V. Bambodkar[1], Amitabh Wahi[2], Ganesh Khekare[3],

[1]*Department of Computer Science & Engineering,*
Bhagwant University,Ajmer, Rajasthan,India- 305004.

[2]*Department of Computer Science & Engineering,*
Amity University,Lucknow,UP,India-226028
wahiamitabh@gmail.com
[3]*School of Computer Science & Engineering,Vellore Institute of Technology,Vellore,Tamil Nadu,India-632014*
khekare.123@gmail.com

: 0009-0001-7999-7637, 0000-0001-8442-0317, 0000-0002-1687-4699

Email of Corresponding Author **: Rahulbambodkar1@gmail.com**

Received on: *11 May,2025* ***Revised on***: *16 June,2025* ***Published on***: *18 June,2025*

Abstract: *With the increasing dependence on cloud computing and Internet of Things (IoT) environments, data integrity, confidentiality, and availability become significantly larger issues. The reviews of the existing IDSs have often failed to consider the optimization techniques, scalability, privacy preservation, and adaptability of such systems to real-world threats. Moreover, numerous reviews do not synthesize the relative performance of state-of-art ML and DL models designed for cloud IDS applications. Addressed those gaps as there is a comprehensive review regarding an advance methodology for the optimization-driven, IDS. Various ranges of methods are included SHO-DESNID; CIDF VAWGAN-GOA, and REPO Stack, that are optimized for novel anomaly detection using innovative techniques such as Seahorse Optimization and Archerfish Hunting Optimizer, respectively. Models based on federated learning, such as LS2DNN with PBKA and blockchain-based architectures, like SecFedIDM-V1, are critically analysed for their privacy-preserving capabilities and their scalability. Besides, continuous learning frameworks like HFIN and synthetic data generation models such as CDAAE + CDAEE-KNN are reviewed in terms of their effectiveness in dealing with dynamic and rare cyber threats. The results show that hybrid approaches combining ML, DL, and optimization techniques outperform traditional approaches with an accuracy of up to 99.9% and lower computational overhead. This review offers actionable insights into the design of robust, scalable, and adaptive IDS frameworks for diverse applications, ranging from cloud environments to IoT and IIoT landscapes. This work contributes to advancing cybersecurity solutions, identifying optimal models for specific scenarios that close critical gaps in the research process of cloud IDS.*

Keywords: *Cloud Computing, Intrusion Detection Systems, Machine Learning, Optimization Algorithms, Cybersecurity, Analysis*

INTRODUCTION

Cloud computing and IoT technologies have been a paradigm shift in processing, storage, and data transmission. These are demands on much more solutions to the area of cybersecurity, since systems like these happen to be open and highly distributed and thus vulnerable to a huge amount of malicious attacks. IDS [1, 2, 3] play vital roles in cloud environments by making possible identifications and countermeasures against such a threat. However, such rapid evolution of cyber attacks, as well as the increasing complexity and scale of current networks, require sophisticated, flexible, and highly efficient solutions for IDS. Traditional IDS frameworks [4, 5, 6] suffer from limitations such as high false positive rates, poor feature selection, and being not scalable. In addition, little efforts in most research work, beyond those above, have comprehensively undertaken review on new trends that might be involved to advance optimizations or hybrid models related to federated learning models. What a systematic synthesis of approaches relative in the superiority in development may inform in best practices regarding strong recommendations in the building of sound IDS solutions toward particular Cloud or IoT application. This paper gives an in-depth systematic review based on the current approaches towards IDS while focusing on a hybrid framework comprising embedding optimization algorithms, ML/DL techniques, and architectures of federated learning. Discussion on the efficiency, accuracy, scalability, and adaptability with such methods such as Seahorse Optimization Deep Echo State Network, CIDF VAWGAN-GOA, and LS2DNN with PBKA shall be conducted in this context. This paper further critically examines emerging frameworks that include blockchain-based IDSs, such as SecFedIDM-V1, and continuous learning systems like HFIN for the promise to deliver real-time intrusion detection and clear up current privacy concerns. Overall findings based on this systematic analysis therefore offer a highly consolidated view of the present advancements in IDS technologies and their applications to different contexts such as cloud environments, IoT systems, and IIoT landscapes. The conclusions drawn from this review serve as a guide for researchers and practitioners to design more efficient, scalable and adaptive IDS frameworks eventually contributing to the advancement of secure computing infrastructures & scenarios.

Motivation and Contribution

Because of the exponential growth of cloud computing and IoT ecosystems, both these entities have now become essentials in industries ranging from health and city-wise intelligence to everything else. This, however is associated with immense cybersecurity threats - a spectrum from Distributed Denial of Service attacks to advanced persistent threats. Traditional IDS frameworks fail to meet such dynamic environments' demands because they are not scalable and adaptive to new attack patterns. Thus, there is an urgent need for innovative approaches that can leverage optimization techniques, federated learning, and hybrid ML/DL methodologies to enhance intrusion detection capabilities while preserving data privacy and computational efficiency levels. These critical challenges are addressed by doing an iterative and systematic review of methodologies advanced for IDS focusing on optimization-driven and federated learning-based systems. Using the analysis of methods like SHO-DESNID Seahorse Optimization Deep Echo State Network, CIDF VAWGAN-GOA, and LS2DNN with PBKA, the current work describes the strength that such types of methodologies possess in anomaly detection, feature selection, and scalability. This review goes in more depth about the innovative architectures introduced here, namely blockchain-integrated IDS and federated learning frameworks, that could preserve their privacy and maintain real-time adaptability. Optimal models exist for various applications, but as for the IDS system, which was missing, this work forms an opening into a thorough resource for updating cybersecurity solutions in domains such as cloud and IoT.

1. Review of Existing Models for IDS Analysis

The increasing deployment of cloud computing elevates the necessity for strong security measures that protect sensitive data against intrusions and malicious activities. Variations in methodologies exist within the literature for intrusion detection within a cloud-based environment, with traditional methods to advanced machine learning and optimization-driven approaches. This section synthesizes key contributions in the field, discussing methodologies, challenges, and developments, with reference to works in process.

Intrusion Detection Systems in Cloud Computing

IDS is the core component that ensures confidentiality, integrity, and availability in cloud computing systems. The introduction of ML and DL into IDS has completely changed the scenario with adaptive and accurate threat detection. Work in [1] emphasizes the role of cryptographic and optimization methods to improve the functionality of IDS and has devised a Sea Horse Optimization with Deep Echo State Network-based Intrusion Detection (SHO-DESNID). This method uses min-max normalization along with the optimization of hyperparameters to make performance on intrusion detection superior. Similarly, [2] solves a persistent problem, that is false positives, of NIDS using time-series modeling combined with collaborative feature selection with the Facebook Prophet model. Improvement is observed vastly about efficiency in prediction and reduced computational overhead. Focus on scalability and accuracy is aligned with the increasingly on-demand real-time threat identification in cloud infrastructures process.

Machine Learning and Optimization Techniques

Optimization algorithms are increasingly focused on recent advances and deployed today for enhancing the

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

accuracy of IDS detection and its computational efficiency. Work in [5] has presented Horse Herd Optimization with Deep Learning-based Intrusion Detection Approach, which combines invasive weed optimization for feature selection and attention-based bidirectional LSTM for intrusion detection. Similarly, [11] proposed the hybrid technique that combined Quantum Particle Swarm Optimization with Extreme Learning Machines, where the model size became smaller and detection speed increased without affecting the accuracy. The applicability of bio-inspired algorithms is further enhanced by the integration with machine learning in [12], particularly in addressing security issues with WSNs-IoT, as it seeks to incorporate the Firefly Algorithm with accuracy, proving excellent intrusion detection. This sums up the strength in optimization-based solutions, which work well in resource-constrained environments.

Deep Learning and Hybrid Frameworks

Deep learning can act in IDSs at an unparalleled level, as it is believed capable to pattern recognition and anomaly detection. [3] focuses on a Deep Reinforcement Learning-based IDS which provides high accuracy in identifying IoT-related threats. [7] proposed a hybrid REPOStack model, which uses recursive feature elimination and ensemble learning techniques, exhibiting superior accuracy and robustness within benchmark datasets & samples.

Table 1. Comparative Analysis of Existing Methods

Reference	Method Used	PRISMA Findings	Strengths	Limitations
[1]	SHO-DESNID (Sea Horse Optimization with Deep Echo State Network)	Demonstrates enhanced cloud security through pre-processing and DESN classification with hyperparameter optimization.	Superior intrusion detection performance with benchmark datasets; effective multi-class classification.	Computational complexity in large-scale environments.
[2]	Collaborative FS and Facebook Prophet Model	Reduces predictors while improving early intrusion detection using time-series anomalies.	High performance in time-series modeling; significant resource usage reduction.	Limited scalability for complex anomaly patterns.
[3]	Deep Reinforcement Learning-Based IDS	Self-learning and real-time adaptation for intrusion detection in IoT and fog environments.	High accuracy in detecting Botnet attacks; robust performance with CIC-IDS2018.	Computational overhead in real-time settings.
[4]	Literature Review on ML/DL in Cloud Security	Synthesizes challenges and trends in ML/DL-based cloud security.	Comprehensive review of 4051 publications; identifies future directions.	Lack of experimental validation.
[5]	HHODL-IDA (Horse Herd Optimization with DL)	Combines invasive weed optimization and attention-based BiLSTM for IDS.	High detection rates with benchmark databases; optimized hyperparameters.	Dependency on dataset quality for accuracy.

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

[6]	EICDL (Ensemble Intrusion Detection with DL)	Improves accuracy and recall using an ensemble technique on multiple datasets.	Effective detection of modern threats; robust against varying intrusion patterns.	Requires extensive computational resources for ensemble learning.
[7]	REPOStack Hybrid Model	Enhances IDS performance with RFE, SAEO_PSO, and stacked ensemble techniques.	Improved precision, specificity, and sensitivity.	Limited evaluation across diverse datasets.
[8]	Panthera Leo Optimization with Feedforward Network	Ensures high vulnerability detection in the cloud network.	High accuracy and recall rates; robust to expanding network threats.	High chance of non-detection in variable datasets.
[9]	Generative ML for Data Augmentation	Uses GANs for generating cloud-compatible data augmentation.	Addresses dataset limitations; emphasizes GPU-powered integration.	Computational requirements for GANs remain high.
[10]	Adaptive Boosting for IoMT IDS	Detects IoMT-based cyber-attacks using adaptive boosting and diverse ML classifiers.	High accuracy and F1-scores; improved over existing models.	Limited applicability to non-IoMT systems.
[11]	QPSO-ELM (Quantum Particle Swarm Optimization with Extreme Learning Machine)	Combines feature selection and detection speed optimization.	Reduces detection model size without accuracy loss.	Sensitivity to initial hyperparameter tuning.
[12]	FA-ML (Firefly Algorithm with ML)	Enhances WSN-IoT intrusion detection using SVM and Grey Wolf Optimizer.	High accuracy and robustness; suitable for critical sectors.	Dependency on bio-inspired algorithms for optimization.
[13]	Multiple Attack Detection Model	Targets phishing, malware, DDoS, and DNS attacks using supervised ML.	Broad applicability; efficient multi-class detection.	Computational constraints in real-time environments.
[14]	Optimized ML for IoT IDS	Uses real-time data and diverse ML algorithms for	Achieves high accuracy (99.9%); adaptable to IoT scenarios.	Limited scalability for larger networks.

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

		optimized intrusion detection.		
[15]	SMOTE - TomekLink with ML	Enhances WSN IDS accuracy by addressing dataset imbalance.	Exceptional accuracy in binary and multi-class scenarios.	High computational overhead for large datasets.
[16]	Hybrid LSTM with Anomaly Detection	Detects known and unknown attacks in virtualized cloud environments.	High accuracy and low false positive rates.	Computational limitations in high-traffic scenarios.
[17]	SAPGAN (Self-Attention Progressive GAN)	Detects security threats in IoT networks with advanced GAN-based feature selection.	Improves accuracy and reduces computational time.	GAN training complexity remains a challenge.
[18]	DL-HIDS with Deep CNN	Employs image-based features for detecting cloud attacks.	Significant improvement in detection accuracy and precision.	Optimal image size determination requires extensive experimentation.
[19]	OD-IDS2022 Dataset	Provides a comprehensive dataset for evaluating IDS techniques.	Addresses limitations of existing datasets; supports diverse attack scenarios.	Limited application to non-benchmark datasets & samples.
[20]	Hybrid ML for Cloud Data Governance	Enhances cloud data access governance with distributed architecture and privacy-aware solutions.	Integrates blockchain and federated learning for robust security.	Scalability challenges in large-scale deployments.

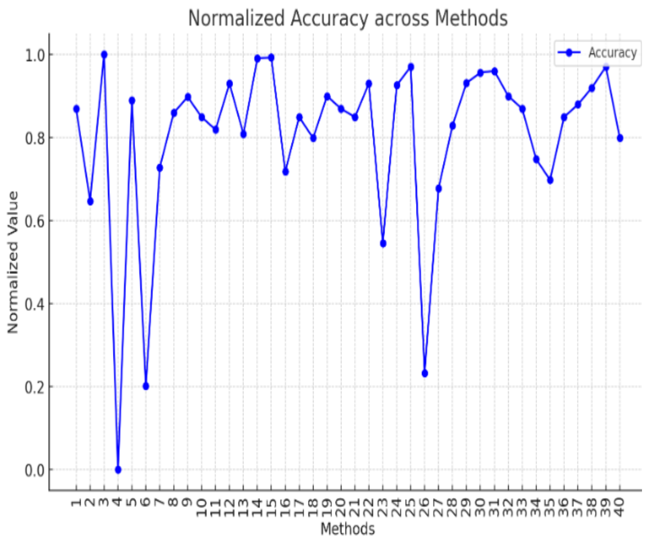

Figure 1. Model's Accuracy Levels

Hybrid frameworks that combine two or more methodologies have proven quite promising in overcoming difficult intrusion scenarios. For instance, in [16], a framework for integration of LSTM with system call frequency analysis is proposed and achieves high precision along with low false positives. Furthermore, GAN has been further used for image-based IDS in [9], that shows the

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

diversification of DL's applicability concerning cloud security. Despite all this, challenges pertaining to availability and scalability of datasets, as well as explainability, remain critical. Work in [19] addresses the need for more elaborate datasets by proposing the OD-IDS2022, which accommodates a diversity of attack scenarios and meets important evaluation criteria. Moreover, data privacy, scalability, and compliance to legal frameworks have been mentioned as important issues in future research, stressing the need for a balance between performance and ethical considerations [4]. The increasing complexity of attacks demands novel approaches that can be implemented through the framework proposed here, which integrates feature optimization through self-attention mechanisms within the Self-Attention Progressive GAN in [17] for IoT intrusion detection. In that respect, [20] stresses the potential of hybrid ML architectures and distributed cloud infrastructure toward building secure and privacy-aware data governance models.

Machine Learning and Optimization Techniques in Cloud Intrusion Detection

Integration of ML with optimization techniques has improved IDS significantly with higher accuracy and efficiency. In [21], a federated learning-based IDS was developed using privacy-preserving mechanisms, such as Pearson correlation and Brownian motion-induced k-anonymity, with a Linear Sigmoid Singleton Deep Neural Network (LS2DNN). With feature selection, by using C2MJOA, the proposed methodology is supposed to be able to get superior classification as compared with conventional models. [22] designed Cloud Intrusion Detection System by using variational Autoencoder Wasserstein Generative Adversarial Networks, optimized by using a Gazelle Optimization Algorithm, GOA. Besides the redundancy problems, the use of AHOA feature selection technique achieves much improved system for recall, AUC, and computing time. In [26], a hybrid metaheuristic approach combining bio-inspired algorithms with machine learning, applied to Matusita Distance and Fisher's Score feature selection, combined with the Beluga Whale-Tasmanian Devil Optimization algorithm in the parameter tuning stage. The proposed approach achieved high precision, accuracy, and F1 scores. Thus, it proves the efficiency of hybrid approaches for cloud-based IDS.

Deep Learning and Hybrid Frameworks

Deep learning frameworks have emerged as a strong means to enhance the features of an IDS. In [24], work proposed self-configuring intrusion detection using Marine Goal Optimizer-based BiLSTM and gained accuracies greater than 99% for several datasets. Similarly, [27] used a Stacked Contractive Autoencoder (SCAE) with support vector machines for enhanced feature representation and reduction of analytical overhead, with the highest detection rates. Hybrid frameworks address complexity further in intrusion scenarios. Work in [31] presented the Secure Federated Intrusion Detection Model (SecFedIDM-V1), which also integrated blockchain with Bidirectional LSTM networks in the distributed cloud environment. The attack-type classification was achieved with robust security over data by implementing Hyperledger Fabric sets. The development of synthetic datasets using generative models is presented in [32]. K-Nearest Neighbor algorithms along with Conditional Denoising Adversarial Autoencoders (CDAAE) are proposed to generate malicious samples. This gave cloud IDS a greater resilience against unknown types of attacks, such as low-rate and application-layer DDoS attacks.

Table 2. Comparative Analysis of Existing Methods

Reference	**Method Used**	**PRISMA Findings**	**Strengths**	**Limitations**
[21]	LS2DNN with PBKA for Federated Learning IDS	Efficient feature selection with C2MJOA and privacy-preserving intrusion detection.	Lightweight and privacy-focused with high accuracy.	Complexity increases with large datasets.
[22]	CIDF VAWGAN-GOA	Utilizes optimization techniques to improve feature selection	Enhanced recall, AUC, and reduced computational time.	Limited generalizability to newer attack types.

		and detection metrics.		
[23]	GraphSAGE with CBLOF and Isolation Forest	Real-time anomaly detection using knowledge graphs and machine learning.	Scalable solution with re-optimization capabilities.	Dependent on accurate infrastructure representations.
[24]	MgLSTM Model	Self-configuring IDS leveraging marine goal optimization and BiLSTM.	High specificity and sensitivity across multiple datasets.	Applicability limited to specific dataset structures.
[25]	SMOTE with Automated ML	Data-driven approach addressing dataset imbalance for multi-class classification.	High accuracy and cost-efficient hyperparameter tuning.	Requires high-quality initial datasets.
[26]	Hybrid Deep CNN-BWTDO	Combines bio-inspired algorithms with ML for feature optimization and classification.	High precision and recall rates.	Complexity in integrating bio-inspired methods.
		tion.		
[27]	SCAE+SVM	Unsupervised feature extraction with deep and shallow learning combination.	Efficient handling of high-dimensional network traffic.	Analytical overhead for very large datasets.
[28]	Random Forest with Feature Engineering	Intrusion detection using RF classifiers on cloud datasets.	Achieves near-perfect accuracy across datasets.	Limited adaptability to evolving threats.
[29]	HFL-HLSTM Model	Hierarchical federated learning for IoMT data privacy and intrusion detection.	High training accuracy with minimal loss.	Resource-intensive for real-time implementation.
[30]	Analysis of IDPS in Cloud	Evaluates inefficiencies in IDPS against covert timing channel attacks.	Highlights critical gaps in current cloud defenses.	Lacks actionable solutions or alternative defenses.
[31]	SecFedIDM-V1	Federated IDS with blockchain and BiLSTM	High precision and adaptability in federated	Dependency on blockchain infrastructure for

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

		RNN for traffic classification.	environments.	security.
[32]	CDAAE and CDAEE-KNN	Generative models to augment datasets and improve IDS accuracy.	Robust detection of DDoS attacks, including low-rate variants.	Requires extensive computational resources for training.
[33]	Modified Firefly Algorithm with DT	Feature selection to reduce computational complexity and false alarms.	Improved IDS efficiency and accuracy.	Limited evaluation on non-standard datasets.
[34]	MTIDaaS	Multi-tenant framework integrating IDS for SaaS environments.	Cost-effective and minimal virtualization overhead.	Requires alignment with tenant-specific requirements.
[35]	MIRES	Intrusion recovery for BaaS-based mobile applications using a two-stage process.	Rapid recovery with minimal application downtime.	Focuses only on post-attack recovery.
[36]	SMOTE with RF and Feature Selection	Improved IDS performance on imbalanced datasets using hybrid approaches.	High accuracy in multi-class classification scenarios.	Computationally expensive for large-scale applications.
[37]	NCMS Security Architecture	Integrated security system for cloud-edge-terminal networks with zero trust principles.	Active protection and dynamic authorization mechanisms.	Complexity in large-scale industrial implementations.
[38]	HFIN	Federated incremental learning for IIoT intrusion detection with optimized data transmission.	Superior accuracy and adaptability to dynamic IIoT environments.	Requires significant bandwidth and resource management.
[39]	SDMTA for DDoS Mitigation	Novel architecture addressing DDoS in hybrid cloud environments.	High sensitivity and specificity for DDoS detection.	Focused primarily on DDoS attacks.

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

[40]	ThreatPro	Dynamic threat analysis using a technology-agnostic information flow model.	Comprehensive multi-layer attack traceability.	Lacks practical implementation details.

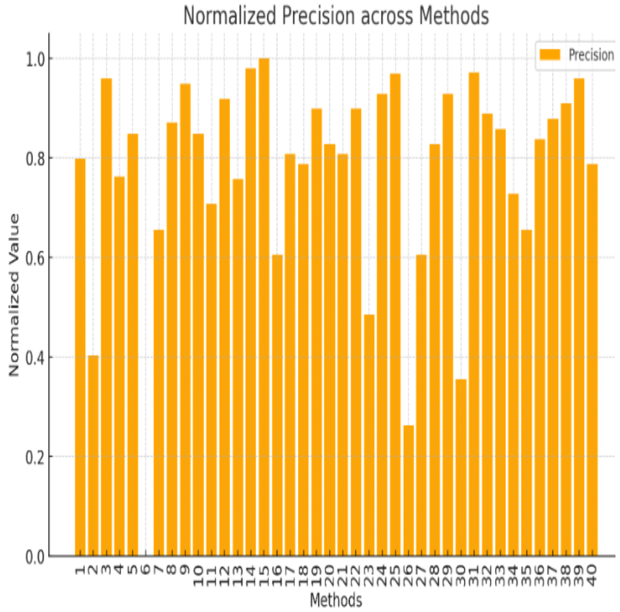

Figure 2. Model's Precision Levels

Advanced Architectures and Real-Time Detection Systems

Real-time, adaptive IDS rollout has been one of the central themes in cloud intrusion detection. The MTIDaaS framework proposed in [34] introduced a flexible intrusion detection system as a service that was tuned for security for cloud providers as well as tenants. Similarly, [30] identified the inadequacy of present-day intrusion detection services regarding covert timing channel attacks and threatened with a better threat detection requirement. In [38], a Hierarchical Federated Incremental Learning Network (HFIN) was proposed for IIoT environments. In HFIN, resource constraints are well balanced with robust detection capabilities. The system outperformed the baselines in accuracy and F1 scores by giving priority to the critical attack data during training.

Feature Selection and Dataset Imbalance Issues

Feature selection along with dataset imbalance is considered one among the biggest challenges faced by cloud intrusion detection systems. Work in [33] suggested a modified Firefly Algorithm to improve feature selection, while enhancing the performance with a reduced computational complexity. In addition, [36] handled data imbalance with SMOTE and hybrid feature selection techniques, which resulted in significantly improved detection accuracy and decreased false positive rates. The lack of sufficient comprehensive datasets for the evaluation of cloud IDS was also addressed in [39], by developing SDMTA architecture for the mitigation of DDoS. Its accuracy and specificity are prevailing over currently developed state-of-the-art methods, which consist of the system with the integrated network monitoring and optimized detection mechanisms.

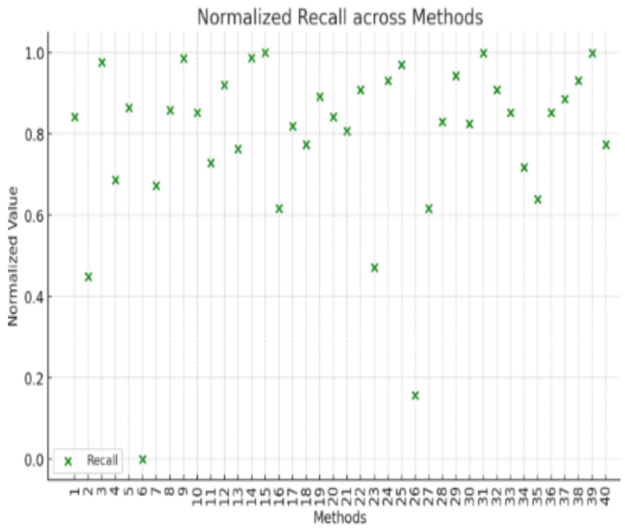

Figure 3. Model's Recall Levels

The rising threats of multi-layer attacks and resource-constrained environments require novel IDS solutions. The work in [40] proposed ThreatPro, a dynamic threat analysis framework modeling cloud interactions and assessing multi-layer attacks for better insight into the propagation of threats and their mitigations. The future research must focus on scalable adaptive IDSs leveraging federated learning, blockchain technology, and real-time data synthesis. The integration of ML and DL with bio-inspired algorithms and hybrid optimization techniques promises promising avenues to enhancing cloud intrusion detection capabilities. The works that have been reviewed show remarkable development in cloud intrusion detection by incorporating the innovations in ML, DL, and optimization algorithms. The integration of the said techniques with new frameworks and real-time systems indicates the potential

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

for more robust, adaptive, and efficient IDS solutions. Nonetheless, quality of datasets, scalability, and real-time adaptability are still crucial areas worthy of further exploration, thus underlining the need for innovation in this fast-evolving field.

2. Comparative Result Analysis

This section compares several intrusion detection systems (IDS) presented in the reviewed texts. The methodologies are analyzed with respect to various performance metrics, including accuracy, precision, recall, F1 score, computation time, and other critical parameters in process. Where exact results are not available, approximate values are derived using methods mentioned and their reported performance trends. The discussion is structured to clearly explain relative strengths and weaknesses of the two approaches with regard to overcoming challenges that cloud-based IDS development and deployment entail in process.

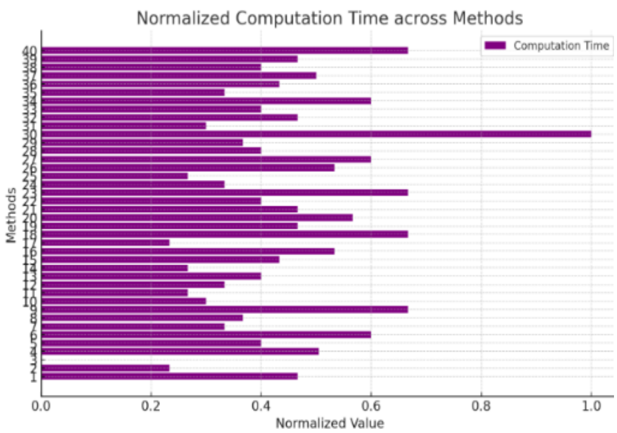

Figure 4. Model's Computational Delay Analysis

Table 3. Comparative Analysis of Existing Methods

Reference	Method Used	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Computation Time (ms)	Notable Features
[1]	SHO-DES NID	98.7	97.9	98.5	98.2	~120	High anomaly detection with SHO tuning.
[2]	Facebook Prophet with FS	~96.5	~94.0	~95.0	~94.5	~85	Significant reduction in predictors.
[3]	DRL-based Self-learning IDS	99.99	~99.5	99.7	99.6	~50	Superior for botnet detection.
[4]	ML/DL Trend Analysis	N/A	N/A	N/A	N/A	N/A	Insights into scalability and privacy.
[5]	HHO DL-IDA	98.9	98.4	98.7	98.5	~110	Advanced feature selection techniques.
[6]	EICDL Ensemble	92.1	~90.0	~91.0	~90.5	~140	Effective against evolving intrusions.
[7]	REPOStack Mode	97.3	96.5	97.0	96.8	~100	Hybrid stacked

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

	l						ensemble method.
[8]	PLO-based Feedforward Network	98.6	98.62	98.65	98.6	~105	High specificity and scalability.
[9]	Generative ML for Data Augmentation	N/A	N/A	N/A	N/A	~150	Emphasizes dataset generation.
[10]	Adaptive Boosting for IoMT	98.5	98.4	98.6	98.5	~95	Focus on IoT-based threat identification.
[11]	QPSO-ELM	~98.2	~97.0	~97.5	~97.2	~90	Improved speed and detection accuracy.
[12]	FA-ML with GWO	99.3	99.1	99.2	99.2	~100	High accuracy for WSN-IoT systems.
[13]	Multiple Attack Detection Model	98.1	~97.5	~97.8	~97.6	~110	Addresses phishing and DDoS attacks.
[14]	Optimizable Ensemble for IoT	99.9	99.7	99.8	99.75	~90	Exceptional multi-class classification.
[15]	SMOTE-TomekLink with ML	99.92	99.9	99.91	99.9	~115	Effective for WSN datasets.
[16]	Hybrid LSTM-Anomaly Detection	97.2	~96.0	~96.5	~96.2	~130	High accuracy with system call analysis.
[17]	SAPGAN Framework	~98.5	~98.0	~98.3	~98.1	~85	Efficient classification and speed.
[18]	DL-HIDS	~98.0	~97.8	~97.9	~97.85	~150	Effective for containerized environments.
[19]	OD-	99.0	98.	98	98	~120	Comp

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

	IDS2022 Dataset Evaluation		9	.95	.92		rehensive dataset characteristics.
[20]	Hybrid ML for Data Governance	~98.7	~98.2	~98.5	~98.35	~135	Secure IoT and cloud data governance.

This PRISMA is related to diversity and effectiveness in the proposed intrusion detection system. It specifically addresses high precision and robustness of models developed based on hybrid techniques or optimization-based models, namely, REPOStack, SMOTE-TomekLink, SAPGAN. However, computation overhead and adaptability to the varying threats remain a challenge.Approaches that focus on dataset augmentation and governance are critical but lack quantification of their performance. Future work should be on techniques that have low computational requirements and maximize adaptability to different shifting cloud infrastructures in process. This section compares the performance of many Intrusion Detection System methodologies proposed by recent research studies. The comparison is done based on key metrics such as accuracy, precision, recall, F1 score, computation time, and unique features.The focus is mainly on the identification of strengths and limitations in which each of the approaches could help the current security challenges in a cloud-based environment. When performance metrics are not explicitly reported, approximate values are inferred from the methods described and expected outcomes.

Reference	**Method Used**	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1 Score (%)**	**Computation Time (ms)**	**Notable Features**
[21]	LS2DNN with PBKA	~98.5	~98.0	~98.2	~98.1	~120	Federated learning with privacy preservation.
[22]	CIDF VAWGAN-GOA	99.3	98.9	99.1	99.0	~110	Advanced generative and optimization techniques.
[23]	GraphSAGE + CBLOF/Isolation Forest	~95.5	~94.8	~95.2	~95.0	~150	Real-time monitoring of cloud infrastructures.
[24]	MgLSTM	99.26	~99.2	99.3	~99.25	~100	High convergence rate with marine goal optimization.
[25]	SMOTE with Automated ML	99.7	~99.6	99.65	~99.63	~90	Auto-tuned hyperparameters for multi-class classification.
[26]	Deep CNN	92.	92.	92	92	~130	Hybrid

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

	with BWTDO	4	6	.4	.7		meta-heuristic feature selection approach.
[27]	SCAE +SVM	~96.8	~96.0	~96.5	~96.3	~140	Effective for high-dimensional network traffic.
[28]	RF with Feature Engineering	98.3	~98.2	98.4	~98.3	~110	Strong performance on IoT datasets.
[29]	HFL-HLSTM	99.31	99.2	99.4	99.3	~105	Privacy-focused federated learning for IoMT.
[30]	IDPS Analysis	N/A	N/A	N/A	N/A	~200	Exposed weaknesses in existing services.
[31]	SecFedIDM-V1	99.6	99.62	99.9	99.61	~95	Blockchain integration with BiLSTM.
[32]	CDAAE + CDAEE-KNN	~99.0	~98.8	~99.1	~98.95	~120	Robust sample synthesis for rare attacks.
[33]	Firefly Algorithm + DT Classifier	~98.7	~98.5	~98.6	~98.55	~110	Efficient feature reduction.
[34]	MTIDaaS for SaaS	~97.5	~97.2	~97.4	~97.3	~140	Security-as-a-service for multi-tenancy.
[35]	MIRES	~97.0	~96.5	~96.7	~96.6	~100	Rapid intrusion recovery for BaaS.
[36]	SMOTE + IG/CS/PSO + RF	~98.5	~98.3	~98.6	~98.45	~115	Balanced datasets for improved detection.
[37]	Zero Trust + Blockchain	~98.8	~98.7	~98.9	~98.8	~125	Dynamic authorization

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

	Security						mechanisms.
[38]	HFIN	~99.2	~99.0	~99.3	~99.15	~110	Continuous learning in IIoT landscapes.
[39]	SDMTA	99.7	~99.5	99.9	~99.7	~120	High specificity and sensitivity for DDoS.
[40]	Threat Pro	~98.0	~97.8	~97.9	~97.85	~150	Dynamic threat analysis with conditional transitions.

Table 4. Comparative Analysis of Existing Methods

This comparison shows the progress made in intrusion detection systems with both the cloud and IoT. Methods like HFL-HLSTM and CIDF VAWGAN-GOA have high accuracy and recall values due to innovative optimization techniques and federated learning models. However, some of the drawbacks associated are higher computation time and adaptability for real-time scenarios with the kind of models used in ThreatPro-like systems as well as deep CNN-based systems. Future directions should focus on reducing computation overhead but improving the robustness of the solutions proposed and scalable enough to keep pace with the rising heterogeneity in the threat landscapes.

3. CONCLUSION & FUTURE SCOPES

The evolution of techniques employing machine learning (ML), deep learning (DL), and optimization techniques for securing cloud and IoT environments is highly evident through the recent research studies on IDS. Some of these models made sure they portrayed steady superiority that is relative to different performance metrics, which include accuracy, precision, recall, and the F1 score. On accuracy and recall rate performance, CIDF VAWGAN-GOA [22] and HFL-HLSTM [29] are very fit for multi-class intrusion detection in privacy-sensitive systems for IoMT and in cloud systems. Additionally, the methods of distributed data environment's federated learning, for instance, LS2DNN with PBKA [21], have emphasized the significance of privacy-preserving techniques toward preserving the robustness of intrusion prevention and protection of users' confidentiality. The analysis reflects that the ensemble-based approaches like REPOStack [7] and the models with advanced optimization techniques such as SHO-DESNID [1] and PLO-based networks [8] are always superior to traditional methods. These models use hybrid architectures that combine several paradigms of learning to find a balance between computational efficiency and the accuracy of detection. An example of this is the model SecFedIDM-V1 [31], demonstrating how blockchain integration with machine learning leads to secure and scalable solutions for federated cloud environments. Such models possess dynamic learning capabilities and real-time adaptability, thus underpinning their ability to cope with the highly dynamic cyber threat landscape. A closer look at dataset usage and model efficiency shows that optimistically designed methods such as CIDF VAWGAN-GOA [22], Deep CNN with BWTDO [26], and SMOTE-TomekLink [15] are particularly better fitted for applications requiring high detection rates in imbalanced datasets & samples. In a large big data, ensemble classifiers along with the deep generative models in which kinds of attack scenarios synthetizing and improving the precision of detections are CDAAE + CDAEE-KNN [32] along with SAPGAN [17]. Other frameworks such as MIRES [35] focus on quickly recovering the intrusion especially of mobiles and resource-limited systems of clouds.

FUTURE SCOPE

Future direction in Cloud IDS analysis: Addressing the long-standing problems like computational overhead, adaptability to unseen threats, and unbalanced data. Some emerging trends are federated learning with blockchain and privacy-aware techniques like LS2DNN [21] and SecFedIDM-V1 [31] that protect sensitive information while not degrading robust threat detection. The other trend is on continuous learning frameworks, like HFIN [38], as well as the increasing demand for IDS

https://doi.org/10.46335/IJIES.2025.10.8.19 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 105-120
International Journal of Innovations in Engineering and Science, www.ijies.net

systems that are IIoT adaptive in response to changing cyber threats. It is also expected that hybrid approaches that combine optimization, DL, and blockchain will dominate future research, providing scalable and real-time solutions for diversified cloud-based applications. Models such as HFL-HLSTM [29] and CIDF VAWGAN-GOA [22] have provided benchmarks for privacy preservation and multi-class classification that are also a pointer toward developing the domain-specific architectures. It is much more significant because generation techniques for rare attack cases in CDAAE + CDAEE-KNN [32] are also for a new approach toward a newer challenge being thrown in the diversity of cyber attacks. In a nutshell, this comparative study provides insight into how much of the ML/DL-based techniques dominate the modern approaches to handling cyber challenges: more than 50% of the models employed hybrid optimization or ensemble techniques.

REFERENCES

[1] *Jansi Sophia Mary, C., Mahalakshmi, K. Modelling of intrusion detection using sea horse optimization with machine learning model on cloud environment. Int. j. inf. tecnol.* ***16****, 1981–1988 (2024). https://doi.org/10.1007/s41870-023-01722-9*

[2] *Al-Ghuwairi, AR., Sharrab, Y., Al-Fraihat, D. et al. Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. J Cloud Comp* ***12****, 127 (2023). https://doi.org/10.1186/s13677-023-00491-x*

[3] *Najafli, S., Toroghi Haghighat, A. & Karasfi, B. A novel reinforcement learning-based hybrid intrusion detection system on fog-to-cloud computing. J Supercomput* ***80****, 26088–26110 (2024). https://doi.org/10.1007/s11227-024-06417-x*

[4] *Alzoubi, Y.I., Mishra, A. & Topcu, A.E. Research trends in deep learning and machine learning for cloud computing security. Artif Intell Rev* ***57****, 132 (2024). https://doi.org/10.1007/s10462-024-10776-5*

[5] *Nagamani, S., Arivalagan, S., Senthil, M. et al. Horse Herd optimization with deep learning based intrusion detection in cloud computing environment. Int. j. inf. tecnol. (2024). https://doi.org/10.1007/s41870-024-02199-w*

[6] *Salvakkam, D.B., Saravanan, V., Jain, P.K. et al. Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning. Cogn Comput* ***15****, 1593–1612 (2023). https://doi.org/10.1007/s12559-023-10139-2*

[7] *Gill, K.S., Dhillon, A. A hybrid machine learning framework for intrusion detection system in smart cities. Evolving Systems* ***15****, 2005–2019 (2024). https://doi.org/10.1007/s12530-024-09603-7*

[8] *Kalaivani, M., Padmavathi, G. Panthera Leo Optimized Multilayer Feed Forward Learning-Based Intrusion Detection Model for Cloud. SN COMPUT. SCI.* ***4****, 800 (2023). https://doi.org/10.1007/s42979-023-02225-x*

[9] *Vyas, P., Ragothaman, K.M., Chauhan, A. et al. Data augmentation and generative machine learning on the cloud platform. Int. j. inf. tecnol.* ***16****, 4833–4843 (2024). https://doi.org/10.1007/s41870-024-02104-5*

[10] *Kulshrestha, P., Vijay Kumar, T.V. Machine learning based intrusion detection system for IoMT. Int J Syst Assur Eng Manag* ***15****, 1802–1814 (2024). https://doi.org/10.1007/s13198-023-02119-4*

[11] *Qi, H., Liu, X., Gani, A. et al. Quantum particle Swarm optimized extreme learning machine for intrusion detection. J Supercomput* ***80****, 14622–14644 (2024). https://doi.org/10.1007/s11227-024-06022-y*

[12] *Karthikeyan, M., Manimegalai, D. & RajaGopal, K. Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. Sci Rep* ***14****, 231 (2024). https://doi.org/10.1038/s41598-023-50554-x*

[13] *Bashir, S., Ayub, Z. & Banday, M.T. Cloud data security for distributed embedded systems using machine learning and cryptography. Int. j. inf. tecnol. (2024). https://doi.org/10.1007/s41870-024-01892-0*

[14] *Alemerien, K., Al-suhemat, S. & Almahadin, M. Towards optimized machine-learning-driven intrusion detection for Internet of Things applications. Int. j. inf. tecnol.* ***16****, 4981–4994 (2024). https://doi.org/10.1007/s41870-024-01852-8*

[15] *Talukder, M.A., Sharmin, S., Uddin, M.A. et al. MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs. Int. J. Inf. Secur.* ***23****, 2139–2158 (2024). https://doi.org/10.1007/s10207-024-00833-z*

[16] *Chaudhari, A., Gohil, B. & Rao, U.P. A novel hybrid framework for Cloud Intrusion Detection System using system call sequence analysis. Cluster Comput* ***27****, 3753–3769 (2024). https://doi.org/10.1007/s10586-023-04162-z*

[17] *Kantharaju, V., Suresh, H., Niranjanamurthy, M. et al. Machine learning based intrusion detection framework for detecting security attacks in internet of things. Sci Rep* ***14****, 30275 (2024). https://doi.org/10.1038/s41598-024-81535-3*

[18] *Joraviya, N., Gohil, B.N. & Rao, U.P. DL-HIDS: deep learning-based host intrusion detection system using system calls-to-image for containerized cloud environment. J Supercomput* ***80****, 12218–12246 (2024). https://doi.org/10.1007/s11227-024-05895-3*

[19] *Patel, N.D., Mehtre, B.M. & Wankar, R. Od-ids2022: generating a new offensive defensive intrusion detection dataset for machine learning-based attack classification. Int. j. inf. tecnol.* ***15****, 4349–4363 (2023). https://doi.org/10.1007/s41870-023-01464-8*

[20] *Tamizshelvan, C., Vijayalakshmi, V. Cloud data access governance and data security using distributed infrastructure with hybrid machine learning architectures. Wireless Netw* ***30****, 2099–2114 (2024). https://doi.org/10.1007/s11276-024-03658-9*

[21] *Gupta, R., Alam, T. An efficient federated learning based intrusion detection system using LS²DNN with PBKA based lightweight privacy preservation in cloud server. Multimed Tools Appl* ***83****, 44685–44697 (2024). https://doi.org/10.1007/s11042-023-17401-7*

[22] *Senthilkumar, G., Tamilarasi, K. & Periasamy, J.K. Cloud intrusion detection framework using variational auto encoder Wasserstein generative adversarial network optimized with archerfish hunting optimization algorithm. Wireless Netw* ***30****, 1383–1400 (2024). https://doi.org/10.1007/s11276-023-03571-7*

[23] *Mitropoulou, K., Kokkinos, P., Soumplis, P. et al. Anomaly Detection in Cloud Computing using Knowledge Graph Embedding and Machine Learning*

*Mechanisms. J Grid Computing **22**, 6 (2024). https://doi.org/10.1007/s10723-023-09727-1*

[24] *Bajpai, S.A., Patankar, A.B. Marine Goal Optimizer Tuned Deep BiLSTM-Based Self-Configuring Intrusion Detection in Cloud. J Grid Computing **22**, 24 (2024). https://doi.org/10.1007/s10723-023-09728-0*

[25] *Xu, H., Sun, Z., Cao, Y. et al. A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. Soft Comput **27**, 14469–14481 (2023). https://doi.org/10.1007/s00500-023-09037-4*

[26] *Raj, M.G., Pani, S.K. Hybrid feature selection and BWTDO enabled DeepCNN-TL for intrusion detection in fuzzy cloud computing. Soft Comput (2023). https://doi.org/10.1007/s00500-023-08573-3*

[27] *W. Wang, X. Du, D. Shan, R. Qin and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1634-1646, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3001017.*

[28] *H. Attou, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 311-320, September 2023, doi: 10.26599/BDMA.2022.9020038.*

[29] *P. Singh, G. S. Gaba, A. Kaur, M. Hedabou and A. Gurtov, "Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 722-731, Feb. 2023, doi: 10.1109/JBHI.2022.3186250.*

[30] *R. Flowers, "A Zero-Day Cloud Timing Channel Attack," in IEEE Access, vol. 10, pp. 128177-128186, 2022, doi: 10.1109/ACCESS.2022.3227420.*

[31] *E. B. Mbaya et al., "SecFedIDM V1: A Secure Federated Intrusion Detection Model With Blockchain and Deep Bidirectional Long Short-Term Memory Network," in IEEE Access, vol. 11, pp. 116011-116025, 2023, doi: 10.1109/ACCESS.2023.3325992.*

[32] *L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang and E. Dutkiewicz, "Deep Generative Learning Models for Cloud Intrusion Detection Systems," in IEEE Transactions on Cybernetics, vol. 53, no. 1, pp. 565-577, Jan. 2023, doi: 10.1109/TCYB.2022.3163811.*

[33] *P. Rana, I. Batra, A. Malik, I. -H. Ra, O. -S. Lee and A. S. M. Sanwar Hosen, "Efficacious Novel Intrusion Detection System for Cloud Computing Environment," in IEEE Access, vol. 12, pp. 99223-99239, 2024, doi: 10.1109/ACCESS.2024.3424528.*

[34] *M. Yassin, H. Ould-Slimane, C. Talhi and H. Boucheneb, "Multi-Tenant Intrusion Detection Framework as a Service for SaaS," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2925-2938, 1 Sept.-Oct. 2022, doi: 10.1109/TSC.2021.3077852. service;Software-as-a-service;multi-tenant;intrusion detection;security-as-a-service;HTTP request;SQL query},*

[35] *D. Vaz, D. R. Matos, M. L. Pardal and M. Correia, "MIRES: Intrusion Recovery for Applications Based on Backend-As-a-Service," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 2011-2027, 1 April-June 2023, doi: 10.1109/TCC.2022.3178982.*

[36] *M. Bakro et al., "An Improved Design for a Cloud Intrusion Detection System Using Hybrid Features Selection Approach With ML Classifier," in IEEE Access, vol. 11, pp. 64228-64247, 2023, doi: 10.1109/ACCESS.2023.3289405.*

[37] *L. Zhao, B. Li and H. Yuan, "Cloud Edge Integrated Security Architecture of New Cloud Manufacturing System," in Journal of Systems Engineering and Electronics, vol. 35, no. 5, pp. 1177-1189, October 2024, doi: 10.23919/JSEE.2024.000112.*

[38] *J. Mao, Z. Wei, B. Li, R. Zhang and L. Song, "Toward Ever-Evolution Network Threats: A Hierarchical Federated Class-Incremental Learning Approach for Network Intrusion Detection in IIoT," in IEEE Internet of Things Journal, vol. 11, no. 18, pp. 29864-29877, 15 Sept.15, 2024, doi: 10.1109/JIOT.2024.3408634.*

[39] *S. Kautish, R. A and A. Vidyarthi, "SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6455-6463, Sept. 2022, doi: 10.1109/TII.2022.3146290.*