A Comprehensive Survey: Integrated AI-Driven Intrusion Detection and Trust-Aware Resource Optimization in Cloud Computing

[1]*Dr.A. Peter Soosai Anandaraj,* [2]*Dr.S.Hemalatha*

[1]*Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia,* [2]*Panimalar Engineering College, Chennai;*

[1]karunya.ieeeproj@gmail.com,[2]pithemalatha@gmail.com

Abstract

Cloud computing has evolved into the core of today's digital world by offering flexible, on-demand computing power for businesses, healthcare, IoT application and distributed services. On the other hand, rapid cloud implementation has introduced security and performance challenges like Cyber Attacks, Distributed Denial-of-Services (DDoS) attacks, threats and inefficient resource utilization. Intrusion Detection Systems (IDS) and load balancing separately failed to enhance trust, adaptability and real-time attack. Most recent research combines Artificial Intelligence (AI), federated learning, block chain, Software-Defined Networking (SDN), trust aware models to improve detection accuracy when optimizing workload distribution. This survey analyses modernization in attack detection systems and trust based optimal load balancing in cloud platforms. This analyses existing method limitation, research gaps and future research towards secure, intelligent and dynamic cloud orchestration systems.

Keywords: AI-based Cyber security, Block chain Security, Cloud Computing, Federated Learning, Intrusion Detection System, Load Balancing, Trust Model.

1. Introduction

Cloud Computing delivers scalable, on-demand resources through shared infrastructures, supporting domains such as healthcare, IIoT, and mobile networks. However, the rapid expansion of cloud [1] ecosystems introduces critical challenges in cybersecurity, trust management, and efficient resource utilization.

Traditional Intrusion Detection Systems (IDS) [2], primarily signature-based, are ineffective against dynamic and unknown threats such as DDoS and insider attacks. AI-driven IDS models improve detection accuracy but suffer from high computational cost, limited scalability, and centralized data dependency. Federated Learning (FL) [3] addresses privacy and scalability concerns by enabling distributed model training without sharing raw data, though it faces communication overhead, synchronization delays, and adversarial vulnerabilities. Blockchain-based IDS frameworks [4] enhance

transparency and decentralized trust but introduce latency, energy consumption, and scalability constraints. A major research gap lies in the lack of integration between intrusion detection, trust evaluation, and resource optimization. Existing load balancing and scheduling mechanisms largely ignore security-awareness and dynamic trust adaptation. This survey highlights the need for an intelligent, unified cloud framework that integrates federated learning, AI-driven detection, blockchain security, and trust-aware resource management to achieve secure, scalable, and adaptive cloud environments.

2. Systematic Review Methodology

This study represents a **Systematic Literature Review (SLR)** to analyse recent advancements in intrusion detection systems, trust load balancing, federated learning, block chain security and intelligent cloud computing frameworks. This approach ensures transparency, reproducibility and reduction of selection bias while identifying significant research contributions. Limitations and future directions.

2.1 Inclusion Criteria

In this review peer-reviewed journal or conference papers addressing security and resources management in cloud computing, IoT, SDN or distributed environments. The works focused on IDS, federated learning security, blockchain based protection, trust management models or load balancing and optimization techniques. This paper provide experimental evaluation, framework design or algorithmic contributions were considered and ensure consistency in analysis

2.2 Exclusion Criteria

This study ensured quality by excluding non-peer-reviewed, duplicate, and irrelevant publications. Papers lacking clear methodology, experimental validation, or technical contribution, as well as studies unrelated to cloud cybersecurity, were omitted from the review.

3. Literature Review

Advancements in cloud computing have research in IDS, federated learning, blockchain security, trust management, and intelligent load balancing. The study analyses and shows centralized security approaches towards distributed cloud protections.

3.1 Screening Phase

In this phase focused databases using keywords related to cloud security, IDS cloud security, IDS, federated learning, blockchain, trust models, and load balancing. The research papers relevant to security or resources optimization used for future evaluation

3.2 Inclusion Phase

In this phase peer-reviewed studies provide clear methodology and experimental results were selected. Federated learning based IDS approaches detection and challenges in communication. Deep Learning IDS models have high detection accuracy and computational resources. Block chain based solutions increased trust and transparency but suffered from latency. Trust management models improve secure access and resource allocation, when load balancing techniques increase system performance but lack of security awareness.

3.3 Contributions of the Survey

This survey provides a comprehensive analysis of recent advancements in cloud security and intelligent resource management by integrating intrusion detection, federated learning, block chain security, trust models, and load balancing mechanisms. The major contributions of this survey are summarized as follows:

1. **Domain-wise Taxonomy:**

This survey provides structured taxonomy that classifies existing research depending upon application domains, including federated intrusion detection, AI-based security, blockchain-enabled protection, trust management frameworks, and intelligent cloud load balancing approaches.

2. Comprehensive Comparative Analysis:

A brief comparative of existing studies analyzing their contributions, performance metrics, achieved results, advantages, and limitations, provides better understanding of recent technological progress.

3. Strength–Limitation Assessment:

The challenges such as computational overhead, scalability issues, communication latency, and lack of real-world deployment for analysing the pros and cons of existing approaches.

4. Emerging Trends Identification:

The emerging trends were federated learning for privacy , blockchain for decentralized trust, AI-driven intrusion detection, and intelligent scheduling for adaptive cloud environments.

5. Research Gaps and Future Directions:

The trust-aware, and integrated cloud security frameworks for supporting scalable and real-time operations.

Table 1.Domainwise Classification

Ref. Area	Application Domain	Methodology	Major Limitations	Identified Research Gap
Federated Learning–Based IDS	IoT, IIoT, Healthcare IoT, Mobile Cloud	Federated Learning (Hierarchical/Clustered FL), Knowledge Distillation, BiLSTM/LSTM	High communication cost, device heterogeneity, synchronization delay	Need for lightweight, adversarially robust, and real-world deployable FL-IDS models
Deep Learning–Based IDS	Cloud, IoT, SDN	CNN, LSTM, Autoencoders, DNN	High training cost, dataset dependency, low explainability	Poor cross-dataset generalization; lack of Explainable AI integration
Blockchain-Enabled Security	Cloud–IoT, Distributed Cloud	Blockchain ledger, Smart Contracts, Consensus algorithms	Scalability issues, latency, computational overhead	Inefficient consensus mechanisms; need lightweight and edge-integrated blockchain
Trust Management in Cloud	Multi-tenant Cloud	Reputation models, SLA-based trust, Trust scoring, Access control policies	Static trust evaluation, policy complexity	Lack of dynamic, AI-driven adaptive trust mechanisms
Secure Load Balancing & Optimization	Cloud Data Centers, Virtualized/Green Cloud	PSO, Reinforcement Learning, SLA-aware & energy-aware scheduling	Limited security integration, scalability constraints	Need integration of IDS with load balancing; energy–security co-optimization

Research Gap

AI-based intrusion detection, federated learning, block chain security, trust management, and cloud load balancing, most existing solutions address the components separately rather than as an integrated system. AI-driven IDS models have drawback such as high computational cost, and limited scalability when federated learning introduces communication overhead and security attacks. Block chain-based

approaches enhance trust however suffer from latency and scalability issues. Added to that recent trust models remain static, and load balancing techniques rarely incorporate real-time security awareness. Hence a key research gap exists in developing a lightweight, scalable, and trust-aware integrated framework that enable IDS and secure resource optimization in dynamic cloud network.

References

[1] M. G. Camila, “A Multi-Tenant Cloud Security Framework Using Zero-Trust Architecture and AI-Based Anomaly Detection,” *American International Journal of Computer Science and Technology*, vol. 6, no. 4, pp. 1–13, Jul. 2024, doi: 10.63282/3117-5481/AIJCST-V6I4P101.

[2] N. Mathivanan and B. Lanitha, “An integrated methodology for intrusion detection and mitigation to optimize cloud security,” *Journal of Cloud Computing*, vol. 15, no. 18, 2026.

[3] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam and O. M. Elkomy, "Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2523-2537, March 2022, doi: 10.1109/TITS.2021.3119968.

[4] Abubakar, A. A., Liu, J., & Gilliard, E. (2023). An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. Electronics Letters, 59(18), e12888,doi.org/10.1049/ell2.12888.

[5] Ceviz, O., Sadioglu, P., Sen, S., & Vassilakis, V. G. (2025). A novel federated learning-based IDS for enhancing UAVs privacy and security. Internet of Things, 31, 101592, doi.org/10.1016/j.iot.2025.101592.

[6] G. Karatas, O. Demir and O. Koray Sahingoz, "Deep Learning in Intrusion Detection Systems," *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Ankara, Turkey, 2018, pp. 113-116, doi: 10.1109/IBIGDELFT.2018.8625278.

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam and M. Shorfuzzaman, "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8065-8073, Nov. 2022, doi: 10.1109/TII.2022.3161631.

[8] Q. -A. Huang and Y. -W. Si, "A Trust-Based Privacy-Preserving Data Retrieval Scheme in Edge-Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2026.3662007.

[9] Mahdi Hosseini, S., Broumandnia, A. & Karimi, R. Blockchain-enabled hybrid evolutionary scheduling for cloud resource optimization. Computing 108, 4 (2026) https://doi.org/10.1007/s00607-025-01574-0.