CINEFORUM
ISSN: 0009-7039
Vol. 66. No. 1, 2026

A Comprehensive Review of Blockchain-Integrated Cloud Security Models

[1]Ashvini Kishan Butani
Research scholar, Computer science
Gujarat Technological University Ahmedabad-382424-Gujarat, India
E-mail: ashbhatti47@gmail.com; ORCID ID: 0009-0002-5656-9741
[2]Dr. Ravirajsinh S. Vaghela
Assistant Professor, School of Cyber security and digital forensics
National forensic sciences University Gandhinagar -Gujarat, India
E-mail: ravirajsinh.vaghela@nfsu.ac.in.; ORCID ID: 0000-0002-6303-9450

Abstract
Cloud Computing is a key technology for making digital ecosystems. Cloud technology has significant benefits for users, but it can also have considerable risks. It can cause significant problems with data safety, hacking, and loss of trust. These problems can come from the way cloud computing is run within centralized control systems. In response to these vulnerabilities, the emergence of blockchain technology has created a decentralized alternative that leverages features such as immutable records, transparent and automated processes created using smart contracts. The following review outlines the emerging state-of-the-art cloud computing security model using blockchain technology through a review of decentralized identity management, provenance tracking, intelligent contract-access control, secure storage frameworks, blockchain-based intrusion detection systems, and decentralized key management systems. A comparative research review indicates that using hybrid Artificial Intelligence (AI)-blockchain solutions, intrusion detection accuracy, trust management reliability and resilience to tampering have been significantly improved. In addition, model performance of Bidirectional Long Short-Term Memory (BiLSTM) blockchain-based frameworks, based on the use of lightweight blockchain-based Convolutional Oversampling Synthetic Neural Network (COSNN) architectures, quantum-assisted encryption, has proven to achieve accuracy rates of up to 99.84%, indicating that the combination of these technologies represents the future of cloud computing security, and offers a platform for future research toward scalable and interoperable privacy-and trust-preserving cloud computing-based-manufactured models.
Keywords: Blockchain Security, Cloud Computing, Intrusion Detection Systems (IDS), Data Integrity, Machine Learning (ML), Deep Learning (DL)

1. Introduction
The foundation of all modern digital systems rests on cloud computing, enabling on-demand computing, scalable storage and access to data via a distributed model, in conjunction with their rapid growth and emergence as a target for cyber-attack [1]. As organizations rely on cloud use, they need clear ways to keep their data safe. Cloud areas that keep changing from new cybercrime threats need strong and firm safety rules [2].

Recently, many academic studies have investigated different methods for securing cloud services. However, most are still dependent upon one or more centralized trust sources for managing various aspects of access control, identity assertion, and governing the information. Centralized systems create points of potential failure, which makes them susceptible to credential theft, escalation of privileges, and tampering with audit logs [3]. Traditional frameworks encounter challenges to ensure the security of resource distributions within diverse networking environments, as well as ensuring verifiably secure data. Constraints such as lack of scalability, lack of current verification of trust, and dependency on third parties prevent traditional architectural frameworks used to secure multi-vendor cloud-complex composites from satisfying requirements for security to be enabled for these types of cloud-complex networks [4].

Due to the characteristics of decentralized and tamper-resistant blockchain technology, it has a logical solution for the issues mentioned. The fact that blockchain technology does not rely solely on a single central authority, and through the process of distributed consensus, blockchain technology creates a lower trust level of a central authority, while increasing resiliency [5]. Blockchain is a method of securely recording data events and user actions. The blockchain is rapidly becoming an essential part of cloud infrastructures as it enhances confidence in data provenance, the secure sharing of resources, and the transparency of audits. Integrating blockchain technology with cloud infrastructure provides a new cloud security model with a focus on a decentralized model with minimal reliance on trust [6].

The review evaluates the blockchain-based cloud security solutions by reviewing the technology. State-of-the-art frameworks would be studied with their strengths and relative weaknesses. The review would explain in detail how the application of blockchain-based cloud security solutions would affect the cloud computing model, identify opportunities to utilize smart contracts as tools for automation of cloud computing security operations, and present a need for the development of an interoperable framework for real-world implementation of cloud computing systems.

1.1 Cloud Security Key Challenges

The most important key challenges of cloud security are:

- **Unauthorized Access and Data Breach -** Sensitive cloud information is exposed to unauthorized access. Risks of credential theft, misconfigured components, and compromised identities are some of the factors that facilitate the persistent and potentially devastating breaches in security measures against sensitive cloud information [7].
- **Insider Threats and Privilege Misuse** - Malicious insiders with legitimate access to sensitive information, evading detection and control, and concealing their actions are among the most challenging threat types to detect [8].
- **Data Security and Tampering Risks** - One of the issues is related to the preservation of data integrity that is stored and processed in the cloud infrastructure, due to its multi-tenant nature and inadequate centralized logging capabilities [9].
- **Lack of Transparency and Trust in Centralized Control** - The traditional cloud architecture model requires centralized organizations to manage all functions which

include user authentication, transaction auditing and the enforcement of company policies. As a result, this architecture creates an individual point of failure and decreases the level of confidence that users have in a decentralized environment [10].

- **Insecure APIs and Misconfigurations** - Poor API security and publicly accessible endpoints are types of vulnerabilities that are suspected to be exploited by an attacker, and can allow an attacker to compromise the authentication, encryption and resource access permission mechanisms [11].

1.2 Blockchain Fundamental Concept for Cloud Security

Blockchain technology uses decentralized architecture to reduce reliance on trust, allowing for greater security for users in the cloud. It is a distributed ledger that keeps track of every transaction across the network. This eliminates the need for a central authority to maintain a database of transactions. Moreover, because the blockchain has been designed to be able to reach a consensus among multiple nodes, an individual node cannot alter its status without first reaching a consensus with other nodes to make changes to the database. This dramatically reduces the risk linked with the existence of a centralized point of failure [12]. The immutable nature of a blockchain can create an irreversible, permanent audit trail documenting all events that occur on any cloud service. The implementation of blockchain technologies allows organizations to build distributed trust management frameworks, enabling the organizations to authenticate their data and safeguard it from tampering in different areas [13]. Through decentralization, immutability, transparency and programmability, blockchain provides an environment in which to address the weaknesses of their current cloud infrastructure and allows for the growth of stronger and safer cloud infrastructures [14].

1.3 Blockchain Integrated Cloud Security Models

Blockchain-cloud security models can decentralize trust through an immutable ledger of information and correct the deficiencies in existing centralized cloud security models. As a result of the development of blockchain technologies, the cloud provides greater strength, trust, and autonomy over the configuration of cloud operations [15]. Blockchain-based cloud security models help improve upon several core areas of focus, including better identity management, improved data integrity, increased security during the sharing of sensitive information, and better ability to monitor complex multi-tenant cloud environments [16].

- **Shared Responsibility Model**
  This model defines the allocation of security responsibilities between the Cloud Service Provider (CSP) and the cloud consumer. CSP's responsibility is to secure the infrastructure, while the consumers secure data, applications, access control, and configuration. Security ownership is clearly defined for each Service Delivery Model (SDM) - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [17].
- **Zero Trust Security Model**
  The concept of zero trust indicates that there are no assumptions made about the safety of an external or internal entity. Each user, device and request must be authenticated, authorized, and continuously validated under a fixed set of guidelines

before encountering resources. To decrease the possibility of attempted attack and lateral movements, it uses IAM-style controls, micro-segmentation, and stringent enforcement of policies [18].

- **Identity and Access Management (IAM) Model**
  IAM ensures that specific individuals get proper access to the cloud resources. This contains the following concepts: authentication, authorization, Single Sign-On (SSO), Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and finally access control in order not to experience unauthorized entry [19].
- **Encryption-Based Security Model**
  This model protects data from compromise with encryption in transit, at rest, and while being processed. Encryption of the data with Symmetric/Asymmetric Encryption Technologies (SAT), Homomorphic Encryption Technologies (HET), and Key Management Systems (KMS) secures the privacy of the data within the cloud environment by providing reliable security controls over the stored data even if communications equipment were compromised [20].
- **Threat Intelligence and Monitoring Model**
  The model is designed to detect, in real-time, threats by finding anomalies using behavior analytics, log management, and automated incident response. Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) tools enhance the visibility that allows users to take proactive steps for security management [21].
- **Virtualization and Isolation Security Model**
  Cloud computing relies a lot on virtualization. Securing each connection point, whether hypervisor, container, etc., and VMs, and providing isolation between tenants is essential for securing cloud data. The separation brought by the virtualization model is strong, and resources in a multi-tenancy cloud setting reduce the risk of events such as VM escape, container breakout, and resource side-channel attacks [22].
- **Compliance and Governance Model**
  The model ensures the cloud follows all regulatory, legal, and organizational policies, such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), International Organization for Standardization (ISO) 27001, National Institute of Standards and Technology (NIST), etc. A compliance and governance model incorporates compliance framework policies, regular risk assessments, and policy enforcement to come up with a secure cloud environment [23].

2. Review of the Past Studies

This section assesses and discusses many research investigations previously undertaken by several authors.

Pawar et al. (2025) [24] proposed a new IDS that incorporated blockchain technology with consensus algorithms along with ML techniques such as XGBoost, Random Forest, Decision Tree, and Random Trees. An Ant Colony Optimization (ACO) method was

adopted to detect network intrusions. The proposed system achieved an accuracy of 99% using NSL-KDD and CICIDS2017 datasets.

Kausar et al. (2025) [25] proposed a safe federated learning framework that uses a private Ethereum blockchain and Homomorphic Encryption (HE) to Detect False Data Injection Attacks (FDIA) in Cyber-Physical Power Systems. To do this, they developed Smart Contracts which authenticate clients and verify the integrity of Model Update Hashes, while allowing for traceability within the system and protecting against unauthorized changes. Testing was conducted using the Cyber-Physical Power System (CPPS) Dataset with XGBoost Long Short-Term Memory (LSTM) and Transformer Models, resulting in Area Under the Curve (AUC) values of 0.94 to 0.96; however, delays related to Blockchain were found to have caused a 13% to 40% increase in training time.

Chauhan et al. (2025) [26] designed the Hybrid DL and Blockchain-based Intrusion Detection System (HDB-IDS) which safeguards Internet of Things networks from cyber threats. The authors used UNSW-NB15 and BoT-IoT as their two primary datasets to create the HDB-IDS system. The researchers made the HDB-IDS system which attained 96.74% accuracy through its BiLSTM Convolutional Neural Network (CNN) architecture that used precision recall and F1 score which measured 95.88% and 94.52% and 95.19% respectively.

Sunanda et al. (2024) [27] developed a novel framework which functioned through Red Fox Optimization (RFO) and Attention-based Bi-LSTM as its main functional elements. The researchers used the NSL-KDD dataset for their study. The system used machine learning optimization methods together with blockchain technology to build its operational framework. The proposed methodology demonstrated its effectiveness through experimental results which achieved approximately 98.9% accuracy on actual IoT datasets.

Sajid et al. (2024) [28] developed a new framework that combined RFO with Bi-LSTM to study the NSL-KDD dataset for detecting IoT attacks. The authors proved their proposed framework operated as a detection system for IoT anomalies through its combination of machine learning and optimization techniques together with blockchain technology. The researchers achieved 98.9% accuracy through their experiments is used actual IoT datasets for testing.

Akbar et al. (2024) [29] created a novel method that secures data transmission between cloud computing systems through Quantum Key Distribution (QKD) and Advanced Encryption Algorithm (AEA). The researchers developed an enhanced Cyber-Security Trust Base Model through their implementation of the Merkle Tree Protocol which they combined with the Multi-Risk Protection Model (MRPM) that uses QKD and Modified Advanced Encryption Standards (MAES) to protect against threats through their new method for Disturbing Image Detection (DID) benchmark dataset analysis. The team achieved an accurate rate of 99.84 percent as their typical performance outcome.

Selvarajan et al. (2023) [30] developed their AI-based Lightweight Blockchain Security Model (AILBSM) to protect privacy rights and security rights of Industrial Internet of Things (IIOT) systems. The researchers applied COSNN for performance testing through various attack datasets while they integrated lightweight blockchain technology with AI

methods. The authors achieved 99.8% accuracy with their Authentic Intrinsic Analysis (AIA) method after completing the process in 0.6 seconds.

Awadallah et al. (2021) [31] created a blockchain-based cloud framework that secures data integrity through the application of Byzantine Fault Tolerance and homomorphic encryption. Master hash values were stored on public blockchains for verification. The study found that Ethereum storage costs 0.005 to 0.010 United States Dollar (USD) per transaction to store a 32-byte hash resulting in an annual expense of approximately 105 USD which makes Ethereum more affordable than Bitcoin.

Qashlan et al. (2021) [32] demonstrated how blockchain technology protects and secures data on cloud computing platforms from cyber-attacks. The researchers tested the study on the NSL-KDD dataset. The researchers tested the developed model through various classification methods. The model achieved an overall accuracy of 95% from their baseline algorithm.

Alkadi et al. (2020) [33] developed a Deep Blockchain Framework (DBF) which provides a secure decentralized intrusion detection system. The authors used an integrated method which combined the BiLSTM DL algorithm with their performance evaluation test of the BiLSTM RNN on University of New South Wales Network-Based 15 Dataset (UNSWNB15) and Botnet of Things (BoTIoT) datasets. The complete accuracy of BiLSTM Recurrent Neural Network (RNN) testing reached 99.41% for UNSWNB15.

Sultana et al. (2020) [34] examined e-health applications that use blockchain technology together with zero-trust security architecture for medical data and image protection. The authors described a trustless and decentralized solution to provide data integrity, encryption, and secure access. Experimental results showed mean retrieval times of 0.75 s for small files, 3.54 s for medium files, and 6.83 s for large files, demonstrating the feasibility of the proposed approach.

Thwin and Vasupongayya (2020) [35] evaluated the performance of a blockchain-based Personal Health Record (PHR) system using data sizes from 128 KB to 32 MB. Results showed that storing 32 MB took 4.84 s and retrieval took 5.19 s, while simulations indicated support for 60,000 daily accesses within 4 minutes, satisfying the 8-minute emergency response requirement. Table 1 shows the comparative analysis of the reviewed literature.

Table 1: Comparative Analysis of reviewed literature.

Author & Year	Objective	Technique Used	Outcome (Accuracy)	Pros
Pawar et al. (2025) [24]	Extend ML for network intrusion detection with blockchain	XGBoost, Random Forest, Decision Tree, Extra Tree, ACO, Blockchain consensus	99%	High accuracy using ACO; blockchain adds trust and immutability
Kausar et al. (2025) [25]	Detect FDIAs in CPPS	Federated Learning + Blockchain + HE	AUC 0.94–0.96	Privacy-preserving, tamper-resistant.
Chauhan et al. (2025) [26]	Secure IoT networks using hybrid DL + blockchain	BiLSTM-CNN, Blockchain	96.74%	Strong performance on IoT datasets; hybrid DL improves detection
Sunanda et al. (2024) [27]	IDS using optimization + attention-based DL + blockchain	RFO, Attention BiLSTM, Blockchain	98.9%	High detection accuracy; efficient optimization-driven model
Sajid et al. (2024) [28]	Hybrid ML–DL model for multi-dataset IDS	XGBoost, CNN-LSTM	98.40%	Good generalization across datasets; strong hybrid performance
Akbar et al. (2024) [29]	Secure cloud data transmission using	QKD, Modified AES, Merkle Tree	99.84%	Very high accuracy; strong cryptographic reinforcement

	quantum + encryption			
Selvarajan et al. (2023) [30]	Lightweight blockchain security for IIoT	Lightweight Blockchain, COSNN, AIA	99.8%	Very high accuracy; low execution time (0.6 sec)
Awadallah et al. (2021) [31]	Cloud data integrity assurance	Blockchain + BFT + HE	(Cost-based)	Low-cost integrity verification
Qashlan et al. (2021) [32]	Data privacy & intrusion detection using blockchain	Blockchain + ML classifiers	95%	Good accuracy; simple yet effective blockchain integration
Alkadi et al. (2020) [33]	Distributed IDS with DL + blockchain	BiLSTM + Blockchain	99.41%	High accuracy for sequential network data using BiLSTM
Sultana et al. (2020) [34]	Secure medical data sharing	Blockchain + Zero Trust	Retrieval: 0.75–6.83 s	Secure and feasible framework
Thwin & Vasupongayya (2020) [35]	Blockchain-based PHR performance	Blockchain-based PHR prototype	Store 4.84 s, Retrieve 5.19 s	Emergency-ready performance

2.1 Comparative Review

The application of ML, DL and blockchain technology to improve the current IDS and security framework accuracy relies on previous research on the improvements found by the implementation of optimization algorithms and blockchain-based technologies, significantly improving network activity detection performance for the detection of network activity anomalies. Models such as (Pawar et al., 2025) [24], (Sunanda et al., 2024) [27], and (Sajid et al., 2024) [28] have justified the greater accuracy produced when applying both ML and DL classifiers used in conjunction with an Optimization method, i.e., Ant Colony Optimization, Random Forest Optimization, and Hybridization of CNN and LSTM models. These models validate the importance of combining optimized feature selection and DL technology to obtain the highest performance efficacy of IDS.

Many investigators examined how to use blockchain with existing IDS technologies to create

transparency, distribute them throughout IDS, thus increasing overall trustworthiness and data integrity throughout the IDS ecosystem. Akbar et al (2024) [29], Selvarajan et al (2023) [30], and Alkadi et al (2020) [33] attained an overall accuracy rate of 99.41% to 99.84% by using blockchain in conjunction with their more sophisticated IDS models, including COSNN model in conjunction with QKD and BiLSTM architecture models as illustrated in Table 2 for comparison purposes to previous research conducted by authors mentioned above.

Table 2: Comparative Analysis

Author & Year	Techniques Used	Accuracy
Pawar et al., (2025) [24]	Random Forest, XGBoost, Decision Tree, Extra Tree, ACO	99%
Chauhan et al., (2025) [26]	BiLSTM-CNN	96.74%
Sunanda et al., (2024) [27]	RFO, Attention BiLSTM	98.9%
Sajid et al., (2024) [28]	XGBoost, CNN-LSTM	98.40%
Akbar et al., (2024) [29]	QKD, Modified AES, Merkle Tree	99.84%
Selvarajan et al., (2023) [30]	Lightweight Blockchain, COSNN, AIA Model	99.8%
Qashlan et al., (2021) [32]	Blockchain with ML Classifiers	95%
Alkadi et al., (2020) [33]	BiLSTM	99.41%

The comparison of accuracy depicted in Figure 1 shows a clear pattern for all hybrid AI regimes that use optimization algorithms and DL models. All hybrid AI regimes examined outperformed all traditional methods. Still, the most crucial factor was that those regimes that included a blockchain-enhanced IDS framework had the highest degree of resistance to overcoming tampering and malicious manipulation. It is also highly likely that there would be a growing trend toward employing AI and blockchain together in developing and deploying next-generation intrusion detection solutions that achieve both the highest levels of accuracy and create robust and decentralized security architectures against threats.

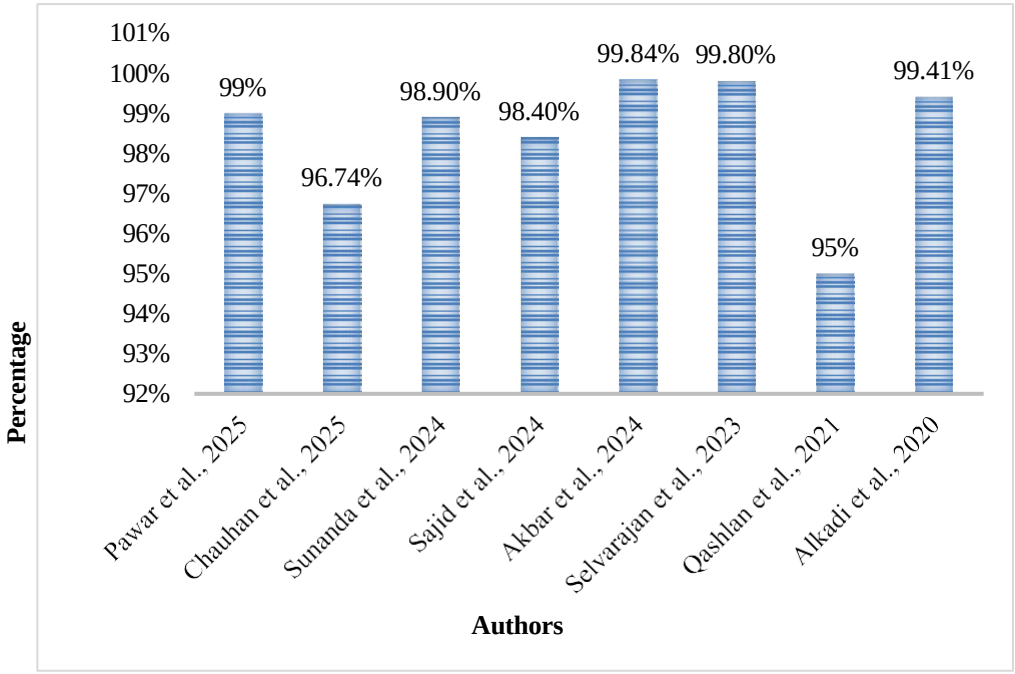

Figure 1: Graphical Representation of Comparative Analysis

2.2 Critical Insights & Research Gaps

This section summarizes key observations from existing studies and identifies open research directions for improving blockchain-enabled AI security frameworks in cloud environments.

- **Trade-offs between accuracy vs scalability**

The AI security models attain their exceptional accuracy through their requirement of high processing power and their capability to handle large data sets which impede their ability to function in real-time situations and to scale throughout vast cloud systems. Blockchain technology establishes trust and maintains data integrity but it requires extra time delays and additional storage space [36].

- **AI model complexity vs blockchain latency**

Advanced AI systems together with deep learning models create better threat detection systems because their development needs extensive computational resources which require long processing durations. The blockchain system introduces extra waiting periods because it needs to complete both transaction validation and consensus processes. Organizations need to achieve a balance between their advanced AI systems and the blockchain technology delays which impact their cloud security response process [37].

- **IDS performance vs real-world cloud constraint**

Although different IDS models demonstrate exceptional accuracy results under control conditions, actual cloud environments present multiple challenges that include bandwidth limitations changing workloads and resource sharing and sensitivity to latency intervals. Such constraints may lead to a decrease in the speed of detection and an increase in the number of false positives or system overhead [38].

- **Security robustness vs smart contract vulnerabilities**

Although blockchain technology improves trust, transparency, and data integrity, smart contracts are susceptible to programming errors, logical bugs, and exploitation attacks. Such weaknesses can be exploited by malicious actors to circumvent security measures, tamper with transactions, or interfere with system functionality. This underscores the importance of formal verification, secure contract development, and continuous auditing [39].

3. Limitations and Challenges

Here are five significant limitations and challenges of blockchain-integrated cloud security models:

- **Scalability Constraints** - The limited throughput and high latency of blockchain technology prevent its use as the main infrastructure system which needs to support multiple cloud computing workloads.
- **High Computational and Storage Overhead** – Existing implementations utilize significant resources for node support, converging on consensus, and maintaining immutable logs.
- **Integration Complexity** - The process of redesigning cloud architecture requires the development of new system skills and the creation of new skills for blockchain implementation in cloud systems and the development of a complicated system that connects different architectural systems.
- **Smart Contract Vulnerabilities** - The process of protecting smart contracts from security threats creates an additional security risk that affects blockchain networks. The method of resolving problems with smart contracts becomes difficult when the contracts contain defects or errors.
- **Regulatory and Privacy Conflicts** - The implementation of cloud systems faces challenges because immutable blocks create problems with legal privacy restrictions that exist in various jurisdictions. The legal requirements that businesses and governments must follow created an essential conflict between these two groups.

4. Conclusion

This survey shows how blockchain technology is integrated with cloud security to achieve decentralized trust, and it also introduces a solution to generate tamper-proof logging, which addresses critical security weaknesses of traditional centralized systems. The reviewed works in this article proved that trust-based solutions could further increase the level of maintaining data integrity in Blockchain-based Cloud Systems (BCSs) despite providing full transparency and higher protection against the least penetrable types of attacks. The study showed that AI techniques can improve the performance of intrusion detection systems due to their capability of detecting attacks in dynamic cloud environments. A study showed that up-to-date hybrid systems employ ML, DL, optimization methods, and blockchain technology to design secure systems with high performance rates. The findings of the study revealed that several factors were limiting their effectiveness, such as technology scalability issues, integration complexities

between systems, varying regulatory regimes, and smart contract security vulnerabilities. Literature reviews provide that blockchain-integrated cloud security paradigm enhances a new opportunity to form a reliable cloud infrastructure which augments the trustworthiness of upcoming cloud computing environments.

5. Future Scope

Future research on blockchain-integrated cloud security models should:

- Develop blockchain architectures that maintain scalability and lightweight design to enable operations in extensive cloud environments while decreasing both latency and computational demands.
- Design adaptive hybrid IDS frameworks by combining blockchain technology with federated learning and reinforcement learning to achieve real-time threat detection while maintaining user privacy.
- To provide interoperability across numerous cloud and hybrid cloud platforms using established blockchain-based security protocols.
- Smart contract security and upgradability improve through formal verification together with automated vulnerability detection and version-controlled contract systems.
- The organization needs to implement privacy-preserving blockchain techniques through zero-knowledge proofs and secure multi-party computation methods to achieve both regulatory compliance and auditing capabilities.
- The system requires implementation of decentralized identity and access management through blockchain technology to support self-sovereign identity and detailed access control within cloud environments.
- Encourage real-world deployment and benchmarking studies to evaluate performance, scalability, cost, and energy efficiency in operational cloud environments.

References

1. Hashim, Wahidah, and Noor Al-Huda K. Hussein. "Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures." SHIFRA 2024 (2024): 8-16. DOI: https://doi.org/10.70470/SHIFRA/2024/002.
2. Reddy, Abhilash Reddy Pabbath. "The role of artificial intelligence in proactive cyber threat detection in cloud environments." NeuroQuantology 19, no. 12 (2021): 764-773. DOI: 10.48047/nq.2021.19.12.NQ21280.
3. Naik, Shivali. "Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy." The Eastasouth Journal of Information System and Computer Science 1, no. 01 (2023): 69-87.
4. Cinar, Burak. "The role of cloud service brokers: enhancing security and compliance in multi-cloud environments." J Eng Res Rep 25, no. 10 (2023): 1-11. DOI: 10.9734/JERR/2023/v25i10995
5. Nasir, Norshakinah Md, Suhaidi Hassan, and Khuzairi Mohd Zaini. "Securing permissioned blockchain-based systems: An analysis on the significance of consensus

mechanisms." IEEE Access (2024). DOI: 10.1109/ACCESS.2024.3465869

6. Owen, John. "Blockchain-Enabled Fine-Grained Access Control and Data Integrity Verification in Distributed Storage Systems." (2025).
7. Akinade, Afees Olanrewaju, Peter Adeyemo Adepoju, Adebimpe Bolatito Ige, and Adeoye Idowu Afolabi. "Cloud security challenges and solutions: A review of current best practices." Int J Multidiscip Res Growth Eval 6, no. 1 (2025): 26-35. DOI: https://doi.org/10.54660/.IJMRGE.2025.6.1.26-35
8. Talekar, Ravikiran. "Insider Threat For Service Account in Google Cloud Platform." (2023).
9. 1 Ang'udi, Janet Julia. "Security challenges in cloud computing: A comprehensive analysis." World Journal of Advanced Engineering Technology and Sciences 10, no. 2 (2023): 155-181. DOI: https://doi.org/10.30574/wjaets.2023.10.2.0304
10. Brown, Jessica, and Stephanie Adams. "The Power of Centralized Security: Best Practices for Managing Security Policies Across Multi-Cloud Environments."
11. Mousavi, Zahra, Chadni Islam, Muhammad Ali Babar, Alsharif Abuadbba, and Kristen Moore. "Detecting misuse of security APIs: A systematic review." ACM Computing Surveys 57, no. 12 (2025): 1-39. DOI: https://doi.org/10.1145/3735968
12. Uddin, Mueen, Anjum Khalique, Awais Khan Jumani, Syed Sajid Ullah, and Saddam Hussain. "Next-generation blockchain-enabled virtualized cloud security solutions: review and open challenges." Electronics 10, no. 20 (2021): 2493. DOI: https://doi.org/10.3390/electronics10202493.
13. Albshaier, Latifa, Alanoud Budokhi, and Ahmed Aljughaiman. "A review of security issues when integrating IoT with cloud computing and blockchain." IEEE Access (2024). DOI: 10.1109/ACCESS.2024.3435845
14. Zhou, Huan, Zeshun Shi, Xue Ouyang, and Zhiming Zhao. "Building a blockchain-based decentralized ecosystem for cloud and edge computing: an ALLSTAR approach and empirical study." Peer-to-Peer Networking and Applications 14, no. 6 (2021): 3578-3594. DOI: https://doi.org/10.1007/s12083-021-01198-z
15. Zou, Jinglin, Debiao He, Sherali Zeadally, Neeraj Kumar, Huaqun Wang, and Kkwang Raymond Choo. "Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges." ACM Computing Surveys (CSUR) 54, no. 8 (2021): 1-36. DOI: https://doi.org/10.1145/3456628.
16. Pasham, Sai Dikshit. "Graph-Based Models for Multi-Tenant Security in Cloud Computing." International Journal of Modern Computing 4, no. 1 (2021): 1-28.
17. Somanathan, Sureshkumar. "Blockchain For Data Integrity In Multi-Cloud Environments: A Project Management Approach." Nanotechnology Perceptions (ISSN: 1660-6795) 20 (2024): 13.
18. Daah, Clement, Amna Qureshi, Irfan Awan, and Savas Konur. "Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework." Electronics 13, no. 5 (2024): 865. DOI: https://doi.org/10.3390/electronics13050865
19. Ghadge, Nikhil. "Analyzing the Role of Blockchain in Identity and Access

Management Systems." Available at SSRN 4872028 (2024). DOI: https://doi.org/10.30574/ijsra.2024.12.1.1019

20. Sasikumar, A., Logesh Ravi, Malathi Devarajan, A. Selvalakshmi, Abdulaziz Turki Almaktoom, Abdulaziz S. Almazyad, Guojiang Xiong, and Ali Wagdy Mohamed. "Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial internet of things." IEEE Access 12 (2024): 12586-12601. DOI: 10.1109/ACCESS.2024.3354846.
21. Meenalochini, P. "Integrated Intelligence Models for Enhancing Cloud Resilience Against Cyber Threats."
22. Khanna, Abhirup, Anushree Sah, Vadim Bolshev, Alessandro Burgio, Vladimir Panchenko, and Marek Jasiński. "Blockchain–cloud integration: A survey." Sensors 22, no. 14 (2022): 5238.b DOI: https://doi.org/10.3390/s22145238.
23. Prabaharan, A. Manoj. "Digital Trust Engineering: A Unified Model Integrating AI, Cybersecurity, And Cloud Governance."
24. PAWAR, Tejaswini, Jyoti RAO, and Pramod PATIL. "Cyber-shield machine learning: an intrusion detection system with blockchain-powered secure log storage across network nodes." *Sigma* 43, no. 3 (2025): 714-725. DOI: 10.14744/sigma.2025.00066.
25. Kausar, Firdous, Sajid Hussain, Karl Walker, and Ayesha Imam. "Blockchain-Integrated Federated Learning Framework for Detecting False Data Injection Attacks in Power Systems With Homomorphic Encryption." IEEE Open Access Journal of Power and Energy 12 (2025): 819-832.
26. Chauhan, Dipti, and Jay Kumar Jain. "Hybrid Deep Learning and Blockchain-Enabled Intrusion Detection System for IoT Networks using Enhanced Dataset Fusion." Journal of Engineering Science & Technology Review 18, no. 4 (2025). DOI: 10.25103/jestr.184.26.
27. Sunanda, N., K. Shailaja, Prabhakar Kandukuri, Vuda Sreenivasa Rao, and Sanjiv Rao Godla. "Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection." *International Journal of Advanced Computer Science & Applications* 15, no. 4 (2024).
28. Sajid, M., Malik, K.R., Almogren, A. et al. Enhancing intrusion detection: a hybrid machine and deep learning approach. J Cloud Comp 13, 123 (2024). DOI: https://doi.org/10.1186/s13677-024-00685-x
29. Akbar, Mohd, Mohammed Mujtaba Waseem, Syeda Husna Mehanoor, and Praveen Barmavatu. "Blockchain- based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing." *Cluster Computing* 27, no. 7 (2024): 9091-9105. DOI: https://doi.org/10.1007/s10586-024-04481-9.
30. Selvarajan, Shitharth, Gautam Srivastava, Alaa O. Khadidos, Adil O. Khadidos, Mohamed Baza, Ali Alshehri, and Jerry Chun-Wei Lin. "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems." *Journal of Cloud Computing* 12, no. 1 (2023): 38. DOI: https://doi.org/10.1186/s13677-023- 00412-y.

31. Awadallah, Ruba, Azman Samsudin, Je Sen Teh, and Mishal Almazrooie. "An integrated architecture for maintaining security in cloud computing based on blockchain." IEEE Access 9 (2021): 69513-69526.
32. Qashlan, Amjad, Priyadarsi Nanda, Xiangjian He, and Manoranjan Mohanty. "Privacy-preserving mechanism in smart home using blockchain." IEEE Access 9 (2021): 103651-103669. DOI: 10.1109/ACCESS.2021.3098795.
33. Alkadi, Osama, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks." *IEEE Internet of Things Journal* 8, no. 12 (2020): 9463-9472.
34. Sultana, Maliha, Afrida Hossain, Fabiha Laila, Kazi Abu Taher, and Muhammad Nazrul Islam. "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology." BMC Medical Informatics and Decision Making 20, no. 1 (2020): 256.
35. Thwin, Thein Than, and Sangsuree Vasupongayya. "Performance analysis of blockchain-based access control model for personal health record system with architectural modelling and simulation." International Journal of Networked and Distributed Computing 8, no. 3 (2020): 139-151.
36. Alhija, Mwaffaq Abu, Osama Al-Baik, Abdelrahman Hussein, and Hikmat Abdeljaber. "Optimizing blockchain for healthcare IoT: a practical guide to navigating scalability, privacy, and efficiency trade-offs." Indonesian J. Electr. Eng. Comput. Sci 35, no. 3 (2024): 1773-1785.
37. Elomda, Basem Mohamed, Taher Abouzaid Abdelaty Abdelbary, Hesham Ahmed Hassan, Kamal S. Hamza, and Qasem Kharma. "An Enhanced Multi-Layer Blockchain Security Model for Improved Latency and Scalability." Information 16, no. 3 (2025): 241.
38. Sefati, Seyed Salar, Bahman Arasteh, Octavian Fratu, and Simona Halunga. "SSLA: a semi-supervised framework for real-time injection detection and anomaly monitoring in cloud-based web applications with real-world implementation and evaluation." Journal of Cloud Computing 14, no. 1 (2025): 38.
39. Alatawi, Mohammed Naif. "Blockchain-Driven Smart Contracts for Advanced Authorization and Authentication in Cloud Security." Electronics 14, no. 15 (2025): 3104.