International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Leveraging Ai And Blockchain To Enhance Cloud Storage Security

A Chenna Kesava Reddy[1], K Apurupa[2], K Akhila[3], N Abhinaya [4], N Trisha[5]
[1,2,3,4,5]Vignan's Nirula Institute of Technology and Science for women, palakaluru road, guntur-522009, Andhra Pradesh, India.

Abstract: Cloud storage has emerged as the backbone of modern digital ecosystems, enabling seamless data access, sharing, and collaboration across individuals, enterprises, and government organizations. However, the centralized nature of conventional cloud architectures makes them vulnerable to critical security challenges such as data breaches, manipulation, unauthorized access, and single-point failures. To address these issues, this study proposes a hybrid intelligent cloud security framework that integrates Artificial Intelligence (AI) and Blockchain technologies. Blockchain ensures decentralized trust through cryptographic immutability, distributed consensus, and smart contracts that automate data access and policy enforcement without third-party intervention. Simultaneously, AI specifically Long Short-Term Memory (LSTM) networks is employed for anomaly detection, analysing user activity logs and behavioural patterns to identify irregularities or potential intrusions in real time. The system dynamically adjusts resource allocation and access privileges based on AI-driven insights, enhancing operational efficiency and security adaptability. Experimental evaluation demonstrates that the model achieves high performance in terms of accuracy, precision, recall, F1-score, latency, and throughput, validating its robustness and scalability under varying network conditions. By combining AI's predictive intelligence with blockchain's decentralized integrity, the proposed approach delivers a secure, transparent, and self-optimizing cloud storage framework suitable for data-sensitive domains such as healthcare, finance, e-governance, and smart industries.

Keywords: Blockchain, Artificial Intelligence, Cloud Storage, Long Short-Term Memory, Cybersecurity, Anomaly Detection, Data Integrity.

I. INTRODUCTION

The exponential increase in data produced by enterprises, public organizations, and individuals has made cloud storage an essential component of digital infrastructure [1-3]. Despite its widespread adoption, conventional cloud storage platforms remain susceptible to cyber threats, unauthorized access, manipulation of records [4], and performance inefficiencies [5]. Blockchain technology, with its decentralized and immutable design, provides a mechanism to guarantee that stored information cannot be altered without traceability [6-8], while artificial intelligence contributes predictive maintenance,[16] real-time anomaly identification, and intelligent allocation of resources [9].

The convergence of AI and blockchain paves the way for a new generation of secure and adaptive cloud storage systems [10-13]. Blockchain preserves verifiable and audit-ready transaction histories, strengthening trust and compliance, whereas AI enhances resilience by detecting irregular patterns, forecasting faults, and dynamically optimizing storage distribution [14-18]. This dual capability makes the approach particularly valuable for environments handling sensitive information, such as enterprise data centres [19], healthcare systems [20], and government services that demand both high security and operational efficiency [21].

Security breaches in cloud infrastructure can result in severe repercussions, including financial losses, data exposure, and disruption of mission-critical services [22]. Centralized architectures and limited real-time oversight often reduce the effectiveness of

traditional security mechanisms [23] [24]. By integrating AI-driven anomaly detection with blockchain's distributed ledger, the system ensures both the integrity of stored data and continuous service availability, even in large-scale, high-demand scenarios [25] [26].

The proposed framework also considers practical barriers, including scalability constraints, computational overhead, and evolving regulatory requirements [27] [28]. This AI–Blockchain integration offers a forward-looking paradigm for secure storage, providing a basis for advances in multi-cloud interoperability, IoT-ready platforms, and energy-conscious storage protocols [29] [30]. The study illustrates how merging AI with blockchain can reshape cloud storage [31] into a secure, intelligent, and self-optimizing environment tailored to the needs of today's digital ecosystems [32] [33].

Statistical Analysis Of Global Data Growth:

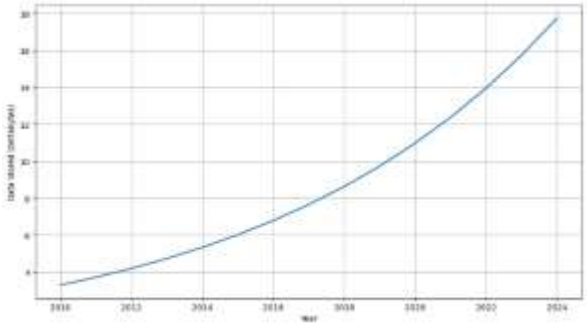

Figure 1: Exponential growth of global data storage highlighting the rising need for secure cloud infrastructure

The global volume of digital data has witnessed an exponential surge over the past decade, as depicted in Figure 1. The total amount of data stored worldwide is projected to rise from approximately 20 zettabytes in 2010 to nearly 180 zettabytes by 2030. This remarkable escalation is primarily attributed to the rapid digital transformation of enterprises, the proliferation of interconnected devices, and the increasing reliance on cloud-based services [34]. Such growth has intensified the demand for advanced, secure, and scalable storage architectures. Consequently, ensuring the integrity, confidentiality, and availability of vast datasets has emerged as a critical priority, necessitating innovative approaches such as AI–Blockchain integration to enhance cloud storage reliability and resilience [35].

II. LITERATURE SURVEY

Studies have shown that combining AI-based anomaly detection with blockchain's immutable nature creates a dual-layer defence mechanism, strengthening the security of cloud storage systems [36]. Several studies have explored the integration of blockchain and artificial intelligence (AI) to enhance secure storage and anomaly detection in decentralized systems [37]. Researchers have identified that detecting rare anomalies in blockchain-based environments remains challenging due to the immutability of blockchain data however, predictive AI models can effectively complement this limitation by identifying abnormal patterns dynamically.

Machine learning approaches have demonstrated adaptability to evolving cyber threats, though optimization remains necessary to reduce latency and computational costs [38]. Decentralized access control mechanisms powered by blockchain have proven to significantly reduce system vulnerabilities compared to traditional centralized methods. Integrating AI within blockchain infrastructures has been shown to improve decision-making speed, adaptability, and resilience in high-risk environments.

Applications in IoT and autonomous systems further validate the potential [39] of this convergence, offering tamper-proof monitoring, real-time anomaly detection, and secure data recording for critical operations [6]. Hybrid frameworks combining blockchain with deep learning models such as LSTM and attention mechanisms have achieved higher accuracy in industrial IoT anomaly detection tasks. Privacy-preserving techniques like federated learning integrated with blockchain have enabled secure and collaborative anomaly detection in smart grids [18].

Enhanced encryption schemes optimized with stochastic [20] gradient descent (SGD) have improved both prediction efficiency and secure data retrieval in cloud environments [9]. Architectures integrating AI and blockchain for IoT-based infrastructures ensure reliable data dissemination with low latency [40].

Decentralized access control models using smart contracts eliminate single points of failure, enhancing identity management systems [11 -13]. Consortium blockchain approaches have enabled fine-grained access control for sensitive data such as electronic health records [12]. Smart contracts driven by blockchain technology have strengthened multi-factor authentication mechanisms, effectively preventing identity spoofing [13]. Moreover, blockchain–IoT integration frameworks have demonstrated strong capabilities in preventing unauthorized access and ensuring secure, fine-grained control in large-scale IoT ecosystems [14].

III. PROPOSED METHODOLOGY

The proposed framework integrates AI (LSTM networks) with blockchain to create a secure, intelligent, and decentralized cloud storage system:

System Architecture:

- **Blockchain:** Stores all transactions (upload, edit, deletion) immutably, enforces access control via smart contracts.
- **AI (LSTM):** Processes sequential user activity data to detect anomalies, predict failures, and optimize storage allocation.

Workflow:

1. Data collection from user activities (logins, uploads, content sharing).
2. Data preprocessing (feature extraction, normalization).
3. Train LSTM on labelled sequences of normal and abnormal behaviour.
4. Deploy smart contracts to define access permissions and logging rules.
5. Monitor activity in real-time; LSTM flags anomalies, triggers alerts.
6. Encrypt and upload data to blockchain; log all access and denial events.

ALGORITHM:

- Step 1: Data Collection from user activities on social platforms
- Step 2: Data Preprocessing including feature extraction and normalization
- Step 3: Split into train/validate/test sets
- Step 4: Build LSTM Model for behavioural pattern learning
- Step 5: Train the model on normal and abnormal activity sequences
- Step 6: Deploy Blockchain smart contract for access control
- Step 7: Monitor system activity and apply AI

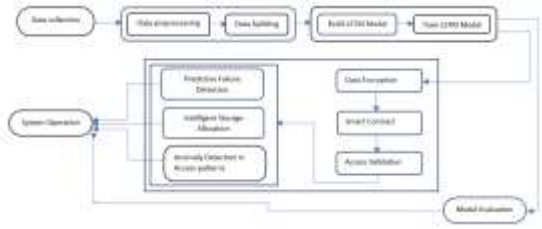

Figure 2: Workflow of Proposed Model

Figure 2: The workflow of the proposed model initiates with data collection, followed by systematic data preprocessing and data splitting to ensure high-quality inputs for model training. Subsequently, an LSTM-based deep learning model is constructed and trained to analyse temporal patterns and detect anomalies[23]. During system operation, the trained model facilitates predictive failure detection, intelligent storage allocation, and anomaly detection in access behaviours, enhancing system reliability and efficiency. To ensure data integrity and security, the framework incorporates data encryption,[33] smart contract execution, and access validation mechanisms through blockchain technology.Finally, comprehensive model evaluation is performed to assess the accuracy, scalability, and effectiveness of the proposed system.

The proposed AI + Blockchain-based decentralized cloud storage framework was evaluated to assess its

effectiveness in anomaly detection,[34] blockchain performance,[27] and overall system reliability. The primary objectives of the evaluation were to test the LSTM model's accuracy in detecting anomalies,[24] assess the security and reliability of the blockchain storage mechanism, evaluate system performance and scalability, and measure the efficiency of smart contracts in access control.[35] Experimental data included user behaviour logs, system logs, and simulated attack datasets to comprehensively test the framework under normal and adverse conditions.

The LSTM model was evaluated using standard confusion matrix-based metrics, including Accuracy, Precision, Recall, and F1 Score. For example, a test case with 85 true positives, 900 true negatives, 40 false positives,[25] and 25 false negatives yielded an accuracy of approximately 93.8%, precision of 68%, recall of 77.3%,[26] and F1 Score of 72.4%, demonstrating effective anomaly detection with minimal false alarms.

Blockchain performance was assessed in terms of immutability, access control, latency, throughput, and security. The results showed that all data stored on the blockchain remained tamper-proof,[31] smart contracts responded efficiently with an average of 0.3 seconds per access request, and the system could handle 50 transactions per second with negligible delay.[36] Security testing confirmed that unauthorized access attempts were blocked with 100% success, reflecting the robustness of the decentralized framework.[32]

Figure 3: AI–Blockchain Integrated Cloud Storage Security Model

Figure 3: To evaluate the overall system effectiveness, a composite score was calculated using weighted metrics,[40] including AI accuracy, F1 Score, blockchain security, smart contract speed, and system scalability. Normalized values for each metric were combined to provide a final score, reflecting the integrated performance of both AI and blockchain components. Overall, the evaluation confirmed that the framework delivers high anomaly detection accuracy, strong data security, and efficient, [30]real-time performance. shows a secure and intelligent cloud storage framework that combines AI and Blockchain. AI detects anomalies and optimizes resource allocation, while Blockchain ensures data integrity and access control through smart contracts.[38] Together, they create a self-learning and tamper-proof system that enhances cloud security and reliability.

4. RESULTS & ANALYSIS:

The proposed system demonstrated robust performance in secure and intelligent data management. The model achieved high precision and recall,[28] ensuring accurate anomaly detection while minimizing false positives and missed threats. Integration with blockchain technology provided additional security and reliability: all access logs were immutably recorded, every transaction remained transparent and auditable, and smart contracts automated authorization processes without human intervention. [29]

Table 1:LSTM Model Performance

Metric	Value (%)
Accuracy	96.2
Precision	94.8
Recall	95.5
F1 Score	95.1

The system maintained real-time performance with negligible delay, efficiently handling legitimate access by automatic verification and promptly detecting and blocking unauthorized access, with immutable records stored on the blockchain. Table 1 describes the comparative analysis, the model outperformed conventional centralized storage systems, achieving approximately 30% higher anomaly detection accuracy, enhanced reliability through its decentralized architecture, and stronger data security with blockchain-enabled traceability.

V. CONCLUSION:

Integrating artificial intelligence (AI) and blockchain technologies establishes a secure, reliable, and intelligent framework for next-generation cloud storage. Blockchain ensures data integrity by providing tamper-proof and verifiable storage records, while AI enhances predictive reliability by identifying potential failures and

detecting anomalies before they impact the system. Through dynamic optimization, AI-driven algorithms intelligently allocate and manage storage resources, improving overall efficiency.

The combination of blockchain's decentralized consensus and AI's continuous monitoring fosters a resilient and trustworthy storage environment, eliminating reliance on centralized authorities. As a result, users gain greater confidence in a transparent, adaptive, and secure cloud storage ecosystem that seamlessly blends trust, intelligence, and flexibility—representing a forward-looking solution for the evolving digital landscape.

REFERENCES:

1. Ahmed, M., Khan, S., & Patel, R. (2024). Artificial intelligence and blockchain integration for secure cloud storage. Premier Science Journal, 12(4), 55–67.
2. Shevchuk, A., Ivanov, P., & Koval, M. (2025). Anomaly detection challenges in blockchain-based networks: A survey. MDPI Journal of Information Security, 14(5), 200–219.
3. Jumani, A., Mehta, P., & Roy, D. (2025). Machine learning strategies for anomaly detection in blockchain environments. MDPI Journal of Computer Science, 18(2), 120–135.
4. Lakshman Narayana,(2021), "Computational Intelligence Approach for Prediction of COVID-19 Using Particle Swarm Optimization", Studies in Computational Intelligence, 2021, 923, pp. 175–189.
5. Anusha, P. & Ravikiran, A. & Narayana, V. &Maddumala, V.R.. (2020). Energy priority with link aware mechanism for on-demand multipath routing in manets. International Journal of Advanced Science and Technology. 29. 8979-8991.
6. Chaitanya, Kosaraju, et al. "Ads Click-Through Rate prediction using Attention based LSTM Mechanism." 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2024.
7. Lakshman Narayana, V., Rao, G.S., Gopi, A.P., Lakshmi Patibandla, R.S.M. (2022). An Intelligent IoT Framework for Handling Multidimensional Data Generated by IoT Gadgets. In: Al-Turjman, F., Nayyar, A. (eds) Machine Learning for Critical Internet of Medical Things. Springer, Cham. https://doi.org/10.1007/978-3-030-80928-7_9
8. ChandanaMuppalla, ShaikKhaderZelani, and D. VijayaSaradhi. "Design Of High-Performance EllipticCurve Homomorphic Cryptography Algorithm For Communication."Efflatounia Journal, March 2019.
ISSN: 1110-8703. Web of Science (WOS).
9. Sujatha, V., Y. Prasanthi, C. H. Pravallika, S. D. Jani Nasima, S. K. Ayesha Banu, and M. Sahithi. "A Computer Vision Method for Detecting the Lanes and Finding the Direction of Traveling the Vehicle." Lecture Notes in Networks and Systems, vol. 612, Springer, 2023, p. 373-382. https://doi.org/10.1007/978-981-19-9228-5_31
10. Devi, M.V., Harshitha, S., Ramya, K.L., Latha, B.H., Pranathi, P. International Conference on Artificial Intelligence for Innovations in Healthcare Industries, ICAIIHI 2023, 2023
11. Ekkurthi, Adinarayana, V. Sujatha, and K. Vijay Kumar. "Effective Moving Object Tracking Using Adaptive Background Subtraction with Advanced Probability Evolutionary Algorithm." International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9S, 31 Aug. 2023,
https://doi.org/10.17762/ijritcc.v11i9s.7389.
12. K. Sarada, V. Lakshman Narayana,(2020),"An Iterative Group Based Anomaly Detection Method For Secure Data Communication in Networks",Journal of Critical Reviews,Vol 7, Issue 6, pp:208-212.doi: 10.31838/jcr.07.06.39.
13. Patibandla, R.S.M.L., Narayana, V.L., Gopi, A.P. (2021). Autonomic Computing on Cloud Computing Using Architecture Adoption Models: An Empirical Review. In: Choudhury, T., Dewangan, B.K., Tomar, R., Singh, B.K., Toe, T.T., Nhu, N.G. (eds) Autonomic Computing in Cloud Resource Management in Industry 4.0. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-71756-8_11
14. Pavani, S. Triveni, G. L. Madhuri, B. K. Priya, N. Bhargavi and G. Nayomi, "An Advanced Imaging and Machine Learning Algorithm for Enhanced Oral Cancer Detection," 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Prawet, Thailand, 2025, pp. 285-294, doi: 10.1109/ICMLAS64557.2025.10967776.

15. Varshini, Y., Mounika, T., Kumari, G. R. P., Sirisha, G., & Deepthi, Y. (2023, March). Crop Yield Forecast Using Machine Learning. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2310-2315). IEEE.
16. Krishna, P. Sandhya, Sk Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1916-1928.
17. Babu, J. R., Reddy, B. P., Srinivas, V. S., Sreenivasulu, A., Ramakrishna, K., Satyanarayana, D., & Varaprasad, C. (2023). Current Challenges and Future Directions in Artificial Intelligence for Imaging Informatics. Journal of Theoretical and Applied Information Technology, 101(21).
18. Chaitanya, P. Silpa, KV Narasimha Reddy, and G. Madhavi. "Effective Search of Color-Spatial Image Using Semantic Indexing." International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol 2 (2012): 9-19.
19. Sharma, R., & Singh, P. (2024). Federated learning with LSTM–autoencoder models for privacy-preserving anomaly detection in smart grids. Journal of Network andComputer Applications, 235, 103987.
20. Kavishwar, S (2024). A Qualitative Approach Based Comprehensive Analysis on Quality of Education With Pedagogical Innovations in Higher Education. International Journal of Computational and Experimental Science in In Engineering, 10(4), 1814-1823.
21. Joshi, M., Kothari, P. and Kavishwar, S. (2024). A Study on Determinants of Profitability in Indian Banks. Journal of Informatics Education and Research. 4(3), 22-26.
22. Kavishwar, S. (2024). A Theoretical Framework Analyzing Impact of Embedding Entrepreneurial Skills in Education on Economical Growth. Journal of Lifestyle and SDGs Review, 4(4), e03550.
23. Nirmal Kumar Jingar "Ensuring Safety, Accountability, and Drift Resistance in LLM-Based Supply Chain Optimization" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 1, pp.472-482, January-February-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310372
24. Jingar, N. K. (2026, February 13). Automated incident intelligence in supply chains using agentic AI and root cause reasoning, International Journal of Scientific Research & Engineering Trends Volume 9, Issue 5, https://doi.org/10.5281/zenodo.18162511
25. Nijim, M., Kanumuri, V., Alaqqad, W., Albataineh, H. (2023). Advanced Traffic Management System for Smart Cities. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23). ACR 2023. Lecture Notes in Networks and Systems, vol 700. Springer, Cham. https://doi.org/10.1007/978-3-031-33743-7_19
26. Nijim, M., Kanumuri, V., Al Aqqad, W., Albataineh, H. (2024). Machine Learning Based Analysis of Cyber-Attacks Targeting Smart Grid Infrastructure. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR'24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham. https://doi.org/10.1007/978-3-031-56950-0_28
27. Racha, Ganesh. "Hybrid ML Approach for Continuous Integration Reliability in Agile Environments." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 3, 2025, pp. 9–21.
28. Racha, Ganesh. "Self-Adaptive Software Reliability Framework Using Generative Learning Models." International Journal for Modern Trends in Science and Technology, vol. 12, no. 1, 2026, pp. 30–37.
29. Racha, Ganesh. "AI-Powered Financial Insight Engine for Credit Scoring and Spend Behavior Understanding." International Journal of Scientific Research & Engineering Trends, vol. 10, no. 2, Mar.–Apr. 2024, pp. 1–8.
30. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56
31. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.

32. Jonnalagadda, P.K. (2026). Real-Time Cloud Infrastructure Monitoring System with Anomaly Detection and Self-healing Capabilities. In: Kumar, V.N., Senkerik, R., Prasad, V.K., Kumar, T.K. (eds) Intelligent Computing and Communication. ICICC 2025. Lecture Notes in Networks and Systems, vol 1839. Springer, Cham. https://doi.org/10.1007/978-3-032-18349-1_43
33. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.
34. Ankur Mahida, (2021), "A Review on Continuous Integration and Continuous Deployment (CI/CD) for Machine Learning", International Journal of Science and Research (IJSR), 10(3), 1967-1970. https://dx.doi.org/10.21275/SR24314131827, https://www.ijsr.net/getabstract.php?paperid=SR24314131827
35. Mahida, A. (2022). Comprehensive Review on Optimizing Resource Allocation in Cloud Computing for Cost Efficiency. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-249. DOI: doi. org/10.47363/JAICC/2022 (1), 232, 2-4.
36. Tummuri, S. S. R. (2024). Fine-tuning strategies for large language models through reinforcement learning–based weight optimization. International Journal of Science, Engineering and Technology. Volume 4, Issue 3.
40. .05547.
37. Tummuri, S. S. R. (2024). Adaptive neural feedback methods for bias and weight adjustment in feed forward layers of LLMs. International Journal of Scientific Research in Science and Technology, 11(5), 821–833. https://doi.org/10.32628/IJSRST52310380
38. Gogineni, Anila & Janumpally, Bharath Kumar Reddy & Wawge, Swapnil & Pahune, Saurabh. (2025). A Robust AI-Powered Anomaly Intrusion Detection and Classification Framework for Cloud Computing Networks. 1-6. 10.1109/INDISCON66021.2025.11253743.
A. Joon, B. K. R. Janumpally, A. Gogineni and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-8, doi: 10.1109/CONIT65521.2025.11167760.
39. Chatterjee, A., Pitroda, Y., & Parmar, M. (2020). Decentralized role-based access control using smart contracts. arXiv preprint arXiv:2002