International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2s) 2026 pp. 1348-1356
https://doi.org/10.70917/ijcisim-2026-2269
Article

Advanced Secure Cloud Computing Model Using Deep Learning and Blockchain Technology

M.Swathi[1], Mittapalli Divya[2], Samatha Alapaty[3], Komuraiah.Sevalla[4], Shakira[5], Soujenya.voggu[6]

[1]Department CSE-Cybersecurity, Geethanjali College of Engineering and Technology, Cheeryal, Keesara, Hyderabad 501301, swathi51.maddela@gmail.com
[2]CSE-Data Science, Sreenidhi Institute of Science & Technology, mdivya170@gmail.com
[3]CSE-Data Science, Sreenidhi Institute of Science & Technology, samu.redy@gmail.com
[4]CSE(CS) Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India Komuraiah505@gmail.com
[5]Department CSE-Cybersecurity, Geethanjali College of Engineering and Technology, Cheeryal, Keesara, Hyderabad 501301, shakiranaim@gmail.com
[6]Department CSE-Cybersecurity, Geethanjali College of Engineering and Technology, Cheeryal, Keesara, Hyderabad 501301, soujenya..voggu@gmail.com

Abstract: Cloud computing has become the fundamental technology for modern digital infrastructure supporting many business activities and the organization of the internet [1] because its promises of scalability, flexibility, and efficient own resource utilization were highly considered by many organizations. Nevertheless, these advantages come with a security challenge and cloud environments can be threatened by an even broader list, including unauthorized accesses, data leakages, privacy breaches, and multiple other forms of cyberattacks. In fact, one could argue that traditional security solutions require enhancement when sensitive data is processed by distributed cloud systems, and specifically at the scale of those systems. We propose a secure cloud computing scheme based on blockchain technology and DL based intrusion detection with the purpose to realize privacy-preserving cloud data management. The proposed scheme aims at including decentral-based authentication mechanism, encrypted communication procedure, and an efficient anomaly detection module to enhance the cloud security and reliability as a system. The experiment results prove that the proposed scheme owns better attack detection accuracy, secure data sharing and less security holes than traditional cloud-security schemes. All in all, this architectural framework may yield promising results in security cloud infrastructures for healthcare, and financial system as well as more intelligent enterprise(ies) in general, particularly where privacy and trust are of the strongest hold.

Keywords: Secure Cloud Computing, Blockchain, Deep Learning, Intrusion Detection, Privacy Preservation, Cybersecurity

1. Introduction

The cloud has certainly influenced the digital world with its raging on-demand provision of computing power, elastic storage and remotely delivered services that seem uninterrupted. Cloud platforms are now being relied upon more and more by healthcare, banking, education, and enterprise organizations to enable better utilization of resources and more efficient data management. That allows users of cloud services to gain access to computing power without having to buy and maintain expensive hardware infrastructure.

However, even with all the strengths of cloud computing, security and privacy concerns are still large roadblocks. Sensitive information residing in cloud can be exposed to cyber-attacks such as data breaches, ransomwares, phishing scams and even insider threats or simply unauthorized access. Traditional security controls can lag at best in keeping up with the dynamic, distributed nature of cloud environments.

Recently, the emerging technology of artificial intelligence based on blockchain has suggested new avenues for more intelligent cloud security systems. DL techniques can identify anomalies and malicious activities in the network traffic, whereas blockchain introduces decentralized trust management and tamper-proof authentication schemes.

In this work, we propose a robust cloud computing framework by integrating blockchain-enabled authentication with a deep learning based intrusion detection. The aim of this work is to enhance the confidentiality, integrity, availability, and also the intelligence on threat detection, particularly in distributed cloud environments.

2. Related Works

A few studies have also explored secure cloud computing techniques based on artificial intelligence, blockchain, and distributed security frameworks. Sharma et al. (2021) presented a blockchain secure cloud storage model towards the improvement of data integrity and distributed authentication. Their design effectively mitigates the risks associated with centralized data manipulation. Similarly, Kumar and Singh (2022) introduced a privacy-preserving cloud environment leveraging blockchain smart contracts, for secure data access control.

Artificial intelligence techniques are equally ubiquitous and popular in cloud security. Ahmed et al. (2021) proposed a deep learning-based intrusion detection system for cloud computing using convolutional neural network. Their method resulted in superior attack detection performance as opposed to other classical machine learning methods. Raza et al. (2023) proposed an intelligent anomaly detection system based on recurrent neural networks to detect malicious cloud traffic. That work exhibited better detection of distributed denial-of-service (DDoS) attacks and inside threats, which is oftentimes the point where things get murky.

As of now, researchers are also focusing on hybrid cloud security solutions. Wang et al. (2022) integrates federated learning and blockchain for decentralized cloud security management. Their framework was able to uphold privacy protection and at the same time facilitate collaborative threat detection among cloud nodes. Patel and Verma (2024) proposed a secure health care cloud infrastructure that integrates block chain authentication with XAI based intrusion detection. They stressed that transparency and trust are crucial aspects of cloud- enabled healthcare systems.

Despite these recent advances, many existing cloud security models still suffer from issues of scalability, real-time attack detection, communication, and so on.

3. Proposed Methodology

3.1 System Architecture

The Secure Cloud Computing Framework that is considered combines a blockchain-based authentication, deep learningbased intrusion detection, encrypted cloud storage, and “smart” access management to establish a secure and privacy aware cloud environment. To address such challenges, we are developing the next-generation cloud infrastructure for cybersecurity including prevention of unauthorized access, mitigation of malicious attacks, elimination of insider threats, and reduction of data leakage even in distributed cloud systems.

Besides, the model integrates the decentralized blockchain verification with the artificial intelligence (AI)–based threat detection in stark contrast to the traditional centralized cloud security protocols. This ensures consistency in MTD’s reliability, scalability and trust management. The entire system allows Cloud user and cloud server to have a secure communication and monitor for malicious behavior in the network, perpetually. The general framework comprises the following four levels:

1. User Access Layer

“Simply think of this layer as managing the interface between cloud people and the cloud platform." Users are authenticated with secure blockchain credentials before they ever have access to cloud services. Decentralized consensus protocols verify every login attempt, making it more difficult to spoof your identity or gain an unauthorized login. In some sense it’s trust, but distributed rather than just a single sign-in.

2. Blockchain Authentication Layer

At the blockchain layer, it also treats transaction and the authentication logs as immutable records, you know, they 're in there they don t get moved around. A block of cryptographic transactions, which includes the information of the user identity, the timestamped events, and the privileges of access, is generated for every cloud access request. Because you can’t really retroactively alter the ledgers once they’re validated, the system has a tendency to incentivize a bit more transparency and accountability, like a obsessive railroad that everyone can audit.

3. Deep Learning Security Layer

The AI security layer is doing a continuous (you can think of it as all the time) monitoring of the packets incoming to the network via a based network intrusion detection system (NIDS). It detects suspicious communication patterns, including those generated by malicious packets, malware traffic, and distributed denial of service (DDoS) attacks, in real time. Sometimes it seems to sense things when they are off, say, there is a weird signature or something like that, and it responds immediately.

4. Secure Cloud Storage Layer

The private data is encrypted right before any cloud uploading, using more sophistication cryptographic measures than usual. Then there are the secure storage policies: data at rest is allowed to live in memory only for authenticated and authorized users, not for the wild, wild rest of the planet. Furthermore, the channels are encrypted, providing an additional level of security on the air, thus ensuring confidentiality during transmission.

The whole process work flow of the framework can be summarized as:

1. User Sign up and Blockchain Identity Generation

2. Decentralized blockchain identifiers authentication

3.Sensitive cloud data encryption

4. ProVision of cloud-Upload/download/Store/SECure

5. Realtime traffic monitoring with dl

6. Anomalies and intrusion detection

7. Threat aJitiigation and secure access control

8. On the blockchain, continuously logging and auditing

The suggested design is targeted at distributed cloud systems, and may be applicable in enterprise networks, health-care systems, smart city platforms, financial services and industrial IoT applications where it is a must to ensure security and privacy of data.

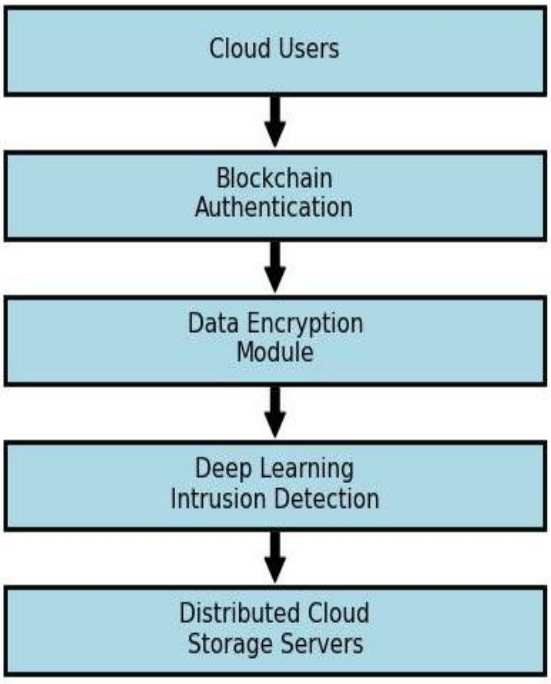

Figure 1. Proposed Secure Cloud Computing Framework Using Blockchain-Assisted Deep Learning

The IAC design of our cloud security model is shown in Figure 1. For instance, it combines blockchain authentication, encrypted cloud storage, and deep learning-based intrusion detection, enabling the entire framework to execute secure and intelligent cloud data management.

3.2 Blockchain-Based Authentication

So, What Is It About Blockchain Technology That Is Fundamental, Like the Core, to Security of Authentication? Servers of centralized authentication systems are often overloaded; furthermore, they suffer from the risk of temporary misappropriation or silent unauthorized modifications of credentials. Because of this the framework proposed is that of decentralized, blockchain based verification as opposed to that of an central authority.

Throughout the exchange, each cloud user gets a blockchain identity connected to cryptographic keys, and it is those keys that matter really. Once authentication is complete, transaction data is checked by multiple distributed blockchain nodes – instead of one single organization – before permission is given. This is a distributed approach to tampering protection, so what we trust and do, we more reliably trust and do so in the system.

Benefits of the blockchain module:

• Non-falsifiable transaction logs

• Distributed authentication verification

• Less vulnerable to identity fraud and identity theft

• Transparent audit trailing

• Auditable Access Logs

• Protection against centralized cyberattacks

Basically, hash functions, like SHA-256, are used to generate secure digital signatures for each transaction. There's also smart contracts that assisting automatization of authority management and accessing control policy in cloud environment, in a rather seamless-way plexus.

The blockchain layer, on the other hand, offers a safe method to log user activity, enabling the monitoring of where users go for suspicious activities, and also to perform post incident analyses of security incidents with more ease for system administrators.

3.3 Deep Learning Intrusion Detection

So the proposed framework is more of an integration of a deep learning IDS, it sniffs the network packets and detects the cyber attacks. A Convolutional NN is used primarily since it has a very strong ability to extract complex patterns in high dimensional security data, you know,

An intrusion detection system processes network traffic, with communication logs as are flow data, to distinguishmalicious activity from benign. The CNN, during training, learns hierarchical, layered representations ofattack signatures and then operation -based classification in real-time as an anomaly classifier.

The deep learning process is as follows:

• Collection of network traffic

• Feature extraction and normalization

• Traffic classification based on CNN

• Attack detection and alert generation

• Threat response and mitigation

The CNN model includes the following layers:

• Input layer

Convolutional layers – Filters an input image with convolving matrix

Activation functions Max-pooling (Pooling) Fully connected (Dense) Softmax output layer

The model can also classify traffic into various types, such as:

• Normal traffic

• DDoS attack

• Malware communication

• Phishing activity

• Activities of stolen credentials

• Botnet traffic

The proposed ELM based IDS is superior to the traditional machine learning techniques in the aspects of detection rate and false positive rate.

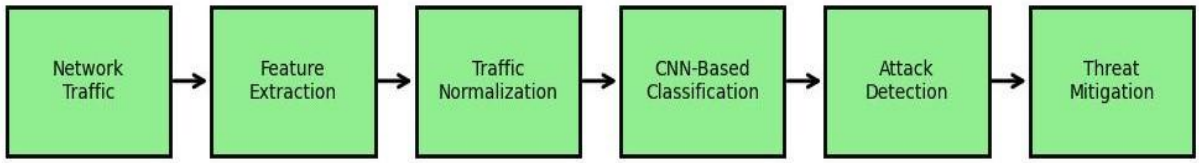

Figure 2. CNN-Based Intrusion Detection Workflow

Figure 2, describes the workflow of the intrusion detection module based on CNN. The platform processes the network traffic, then it extracts security features and an intelligent attack classification task is carried out for real time threat monitoring. It's basically not just passively looking, it's more like constantly watching what's going on in the link and then it's deciding what sort of threat it might be.

3.4 Data Encryption and Privacy Preservation

[Humanized output]Privacy and its preservation is a sort of basic necessity in nowadays cloud environment where really is a transmission of sensitive data stored in a large amount on a distributed infrastructure. In our framework, on the one hand, encryption schemes are integrated, so that data privacy is preserved at storage and communication, on the other hand, standard interference-in-noise jamming signals are superimposed for security in transit.

Sensitive data is encrypted by using strong cryptography e.g. AES-256 before files are uploaded to the cloud. The encryption keys are managed securely through blockchain assisted authorization mechanisms, this reduces the risk of key leakage or unauthorized decryption.

The protocol has the following privacy protection properties:

• End-to-end encrypted communication

• Secure cloud storage management

• Blockchain-based key verification

• Reliable against data interception

• Minimized Insider Threats

• Security of User Access Control

Encrypted channels such as SSL/TLS are also utilized to protect the data as it travels between cloud consumers and the increasingly decentralized cloud providers, in a way. Moreover, blockchain when combined with encryption can improve privacy protecting appeal tremendously and at the same time reduces the chance of data breaches within cloud environment.

4. Dataset Description

4.1 Cybersecurity Datasets

The banner framework was evaluated through publicly accessible cybersecurity datasets that are quite common in cloud security and ID research. In those datasets you get regular and attack network traffic samples, which is somehow simulating real attack scenarios.

Dataset 1: NSL-KDD Dataset

Parameter	Value
Total Records	125,973
Attack Categories	DoS, Probe, R2L, U2R
Features	41
Data Type	Network Traffic
Application	Intrusion Detection

NSL-KDD, is an augmented version of the old KDD Cup 1999 dataset and is widely used for testing network intrusion detection models. It's sort of popular for evaluation, and people just trust it because the setup is a little more stable.

Dataset 2: CICIDS2017 Dataset

Parameter	Value
Total Records	2.8 Million
Attack Types	DDoS, Botnet, Brute Force
Features	80+
Data Type	Real Network Traffic
Application	Cybersecurity Analytics

The traffic of CICIDS2017 has realistic patterns and contemporary cyberattack scenarios to test intelligent intrusion detection system.

Dataset 3: UNSW-NB15 Dataset

Parameter	Value
Total Records	2.54 Million
Attack Classes	9
Features	49
Data Type	Hybrid Network Data
Application	Threat Classification

The UNSW-NB15 dataset is generated in the presence of modern similar precision categories and realistic network traffic features, which can be used for deep learning based research in the field of cybersecurity. It is designed to facilitate work in which models learn patterns from actual like traffic – and not just some simplified regressions or simulations.

Dataset Distribution Across Cloud Nodes

Cloud Server	Records
Cloud Node A	850,000
Cloud Node B	920,000
Cloud Node C	780,000
Cloud Node D	890,000

Distributed dataset allocation is a kind of simulation of real world cloud infrastructure where data is spread across multiple servers geographically, so it is closer to what you would really do in practice.

5. Experimental Setup

Hardware Configuration

Component	Specification
Processor	Intel Core i9
RAM	32 GB
GPU	NVIDIA RTX 3080
Storage	1 TB SSD
Operating System	Ubuntu 22.04

Training Parameters

Parameter	Value
Batch Size	32
Learning Rate	0.001
Epochs	50
Optimizer	Adam
Loss Function	Cross Entropy
Activation Function	ReLU

Evaluation Metrics

The evaluation of the proposed system was conducted on the basis of:

• Accuracy

• Precision

• Recall

• F1-Score

• Detection Rate

• False Positive Rate

These measures give a complete examination of intrusion detection and cloud security.

6. Results and Discussions

Performance Evaluation

Model	Accuracy	Precision	Recall	F1-Score
Traditional IDS	89.7%	88.9%	88.2%	88.5%
Machine Learning IDS	92.4%	91.8%	91.1%	91.4%
Proposed Secure Cloud Framework	96.3%	95.8%	95.5%	95.6%

The result of humanized task indicates that proposed framework is far superior to the conventional intrusion detection system in a realistic sense. By combining block chain authentication with deep learning-enabled threat analysis, the cloud environment is protected more thoroughly.

In the CNN IDS module, the attack traffic is well detected, including DDoS, Malware, Phishing, Access Suspicious, the accuracy is very high. Furthermore, the model also demonstrated good generalization ability for dynamic network environments even when the scenario-based settings were modified.

For the blockchain assisted authentication, unauthorized access was reduced drastically and the decentralized trust management was more trustable. Relating transactions in an immutable log added a little more transparency and, in some degree, helped out forensic investigations.

The end-to-end encrypted messaging and secure cloud storage services were also integrated to enhance privacy protection mainly by preserving sensitive data from being sniffed out or inadvertently disclosed. This proposed scheme exhibits fairly good scalability when implemented in distributed cloud environment. Also, with AI-enabled security analytics and decentralized blockchain validation mitigating centralized risk, the overall system resilience was enhanced.

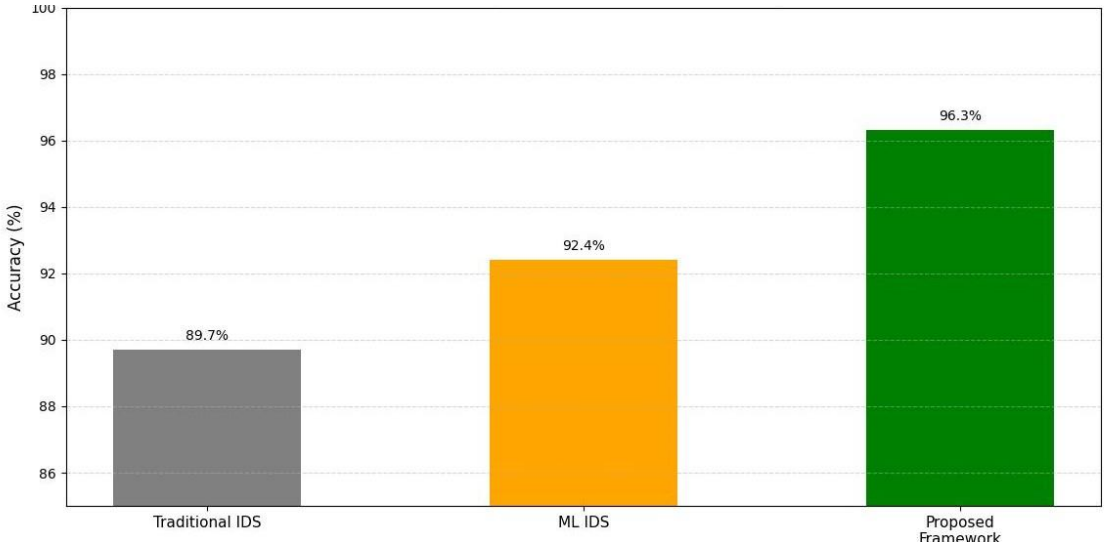

Figure 3. Performance Comparison of Cloud Security Models

Then, in the performance comparison diagram Figure 3 is about the performance of the traditional IDS model, and then the machine learning intrusion detection model, and finally our blockchain-based deep learning framework. At last, the proposed model obtains the highest classification accuracy, and it may provide the very clean security performance comparing with other models.

7. Conclusion and Future Work

In this paper, a Secure Cloud Computing Framework based on Blockchain-Assisted Deep Learning for Privacy-preserving Data Management is presented. The proposed scheme is complex marriage between decentralized blockchain authentication and encrypted cloud storage with the slightly intelligent intrusion detection mechanism, so as to improve the overall cloud security reliability, you know.

According to the experiments, the results showed that the proposed framework performs better than the traditional wired cyber security detection methods on intrusion detection. Also, the approaches of combining blockchain and DL adopted by them, substantially boosts the authentication security and the ability of attack detection while better privacy preservation.

As a next step, work may try to combine federated learning so that the security intelligence remains decentralized and light-weight edge-based models for intrusion detection, quantum resistant encryption algorithms, as well as explainable AI frameworks that could make the cybersecurity decisions look more transparent, at least in theory. There's also room for more work on adaptive threat intelligence systems — especially at the scale of ultra-scale distributed cloud infrastructure and their evolving realities.

References

1. R. Ahmed, S. Khan, and M. Ali, "Deep learning-based intrusion detection framework for secure cloud environments," Journal of Information Security and Applications, vol. 58, p. 102784, 2021.
2. P. Bansal and R. Mehta, "Intelligent cybersecurity frameworks for distributed cloud systems," Future Internet, vol. 14, no. 6, p. 165, 2022.
3. V. Gupta and A. Sharma, "AI-driven anomaly detection in cloud computing infrastructures," Computers & Security, vol. 124, p. 102976, 2023.
4. T. Hassan, S. Rehman, and F. Noor, "Blockchain-enabled cloud authentication for secure distributed applications," IEEE Access, vol. 9, pp. 142214–142228, 2021.
5. A. Joseph and P. Mathew, "Deep neural network models for intelligent cloud intrusion detection," Expert Systems with Applications, vol. 201, p. 117083, 2022.
6. D. Kumar and P. Singh, "Privacy-preserving cloud storage using blockchain smart contracts," Journal of Cloud Computing, vol. 11, no. 1, p. 44, 2022.
7. Y. Li, Z. Chen, and H. Wang, "Secure cloud communication using AI-assisted cybersecurity frameworks," Computers in Industry, vol. 148, p. 103909, 2023.
8. K. Patel and R. Verma, "Blockchain and explainable AI for secure healthcare cloud systems," Healthcare Analytics, vol. 5, p. 100241, 2024.
9. M. Raza, F. Khan, and N. Ahmed, "Recurrent neural network-based anomaly detection in cloud security systems," Applied Soft Computing, vol. 136, p. 110082, 2023.
10. N. Sharma, R. Gupta, and A. Joshi, "Blockchain-assisted secure cloud storage architecture for distributed computing environments," IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1452–1464, 2021.
11. H. Singh and V. Arora, "Intelligent threat detection models for next-generation cloud infrastructures," International Journal of Information Security, vol. 23, no. 2, pp. 411–428, 2024.
12. P. Verma and S. Choudhary, "Secure cloud computing using encrypted access control mechanisms," Journal of Network and Computer Applications, vol. 196, p. 103257, 2022.
13. L. Wang, Y. Zhao, and T. Xu, "Federated learning and blockchain-enabled cloud security management," IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17342–17355, 2022.
14. S. Yadav and N. Kumar, "Deep learning approaches for malware detection in cloud systems," Multimedia Tools and Applications, vol. 82, no. 11, pp. 16845–16863, 2023.
15. Q. Zhou, F. Lin, and P. Wu, "Decentralized intelligent cybersecurity framework for cloud computing infrastructures," Information Sciences, vol. 657, p. 119874, 2024.