Grenze International Journal of Engineering and Technology, June Issue

Enhanced Security in Cloud Applications using Blockchain

Mathiazhagan Mani[1], Divya Midhun Chakkaravarthy[2], Janani Selvam[3], Amiya Bhaumik[4] and Kesava Sundara Nathan[5]
[1]PhD Research Scholar, Faculty of Engineering, Lincoln University College, Kota Bharu, Kelantan, Malaysia
[2-4]Professor, Faculty of Engineering, Lincoln University College, Kota Bharu, Kelantan, Malaysia
Email: janani@lincoln.edu.my
[5]Research Scholar, Faculty of Electrical and Electronic Engineering (FKEE), Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja, Johor, Malaysia

***Abstract*— The cloud computing paradigm revolutionized technology by providing an efficient and easily accessible medium to gain access to IT resources. Security and privacy still remain serious challenges as far as cloud computing is concerned. The present write-up focuses on securing cloud applications with blockchain technology and integrating them into cloud computing. Our study presents how the main vulnerabilities in Cloud of Things (CoT) environments are addressed by blockchain's decentralized, immutable, and public architecture. We study decentralized security measures along with access control methods and privacy protection mechanisms, including differential privacy, k-anonymity, and attribute-based access control. An exhaustive analysis of BaaS implementations is given to show that the integration leads to shared trust in third parties, no ability of data tampering, and an increase in fault tolerance. Experiments showed that the proposed blockchain-based scheme provides a significant increase in confidentiality, integrity, and authenticity in a cloud environment while still being scalable. This paper adds to understanding how distributed ledger technology can be a successful countermeasure to cloud security risk in IoT-enabled applications.**

***Index Terms*— Blockchain, Cloud Computing, Data Security, Privacy Preservation, Distributed Systems, Access Control, Cloud of Things, Cyber Security.**

I. INTRODUCTION

A. Background and Motivation

Blockchain techno is a disruptor in offering safe digital contracts among peers without the interference of a third-party. A blockchain is a public distributed ledger in which exchanges are recorded with an inviolable design and hence it becomes impossible to hack the financial transactions concerning the digital currency [1]. In a centralized database, the changes made to such data are arbitrary; hence blockchain has more rules for validation and guarantees security through cryptographic schemes.

Adoption of cloud computing has occurred for many areas of information technology, primarily due to its efficiency, ease of use, and resource optimization. Cloud security and privacy, mainly confidentiality, integrity, authenticity, access control, and data protection, are some of its main concerns. The combinatorial architecture of the blockchain and cloud computing marks a departure from the state-of-the-art secure architecture trend [2].

Grenze ID: 01.GIJET.12.2.80_23

B. Problem Statement

There are three main dangers associated with CoT built in conventional ways. By its structure, the central mode of communication provably harms scalability as IoT networks begin to expand. Thirdly, the existing systems need third-party cloud providers to be trusted in processing IoT data, thus creating information security vulnerabilities for existing CoT systems. Fusion of networking and centralized architectures produces communication latencies, which eventually means more energy consumption on IoT devices for large-scale, practical CoT deployments [3][4].

C. Proposed Solution

With BCoT, which stands for Blockchain-based Cloud of Things, the paper proposes to offer an end-to-end solution for cloud security.
By bringing the decentralized architecture of blockchain to cloud computing, we solve scalability, trust, and latency problems while enhancing the actual security mechanisms-such as evidence by distributed validation and immutable record-keeping as well as cryptographic protection.

D. Key Contributions

(1) Comprehensive appraisal of the blockchain-cloud integration for security improvements; (2) privacy-preserving model investigations, including differential privacy and k-anonymity; (3) blockchain-based access-control mechanism evaluations; (4) performance evaluations showing Mean Absolute Error (MAE) and Mean Relative Error (MRE) improvements; and (5) practical insights into the BCoT implementation in smart healthcare, smart cities, and IoT-enabled applications.

II. CLOUD COMPUTING FUNDAMENTALS

A. Cloud Service Models

Cloud services are categorized into three primary models:

- Infrastructure as a Service (IaaS): This provides computing capabilities, storage, and hardware with data protection, management, and backup services.
  The applications and data are the responsibility of the user while the infrastructure is managed by the provider [5].
- Platform as a Service (PaaS): They help in the development of applications and run them without really having to worry about the coding, architecture, and the inventory underneath; therefore, they take the load off from development [6].
- Software as a Service (SaaS): Application access enables user resources to be cloud-based while adhering to reduced administration overheads as compared to the traditional way of installation on-premise [7].

B. Cloud Deployment Models

- Public Clouds: Several users access applications and web services months through the internet. These resources are isolated for each user, and the management of third-party service providers in all aspects of privacy and security concerns. Users cannot establish management themselves over the cloud infrastructure [8].
- Private Clouds: Total Control over managing and securing data is exercised by organizations at an exorbitant investment, but they provide better trust and governance [9].
- Community Clouds: Several organizations have come together for common aims and requirements in order to build a shared cloud infrastructure.
- Hybrid Clouds: Combine private and public cloud platforms, connecting private clouds with multiple peripheral services while enabling authorized users to access information through diverse channels [10].

C. Cloud Computing Advantages

Cloud computing offers significant benefits:

- cost reduction through economies of scale,
- disaster management via secure data backup and recovery,
- green computing with reduced electronic waste,
- easy management requiring minimal IT overhead and
- uninterrupted service availability with low disruption rates [11].

III. BLOCKCHAIN TECHNOLOGY ARCHITECTURE

A. Blockchain Fundamentals

A public, distributed, unalterable database built on peer-to-peer network models where transaction data is not managed by any centralized authorities, is the peer-to-peer distributed database known as blockchain. Transactions will be stored in immediately sequenced blocks, accessible in a reliable way at any time by any user of the blockchain network [12].

Consensus mechanisms and cryptography validate transactions the blocks are chained with tamper-resistant and modification-resisting properties.

B. Blockchain Characteristics

- Decentralization: Eliminates single points of failure and requirements for trusted third parties. All network members validate IoT data and ensure immutability through equal rights and peer-to-peer architecture [13].
- Privacy and Security: In fact, blockchain smart contracts enable full automation of authorization for cloud services and IoT processes avoiding security problems and supporting fine-grained data regulation; users basically maintain control over all personal interactions and accesses with their data. [14][15].
- Collaboration: It creates an open ecosystem in which cloud providers and IoT customers can cooperate while providing confidence to multi-parties in collaboration and information sharing, without preceding them with reporting or placing trust in intermediaries. [16].

C. Cloud of Things Enhancement

CoT systems integration to the blockchain has the following benefits:

- Scalability Support: Cloud infrastructure includes robust processing capabilities, thereby expediting the transaction execution in the blockchain and allowing computation resources on demand through federation cloud systems [17].
- Fault Tolerance: The principle of replication in cloud infrastructures maintains the replicated blockchain data across all those interconnected systems and reduces the risk of a single point of failure, thus continuing operations in case of server attack or component malfunction [18].

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

A. Data Security and Privacy

Risks are being carried because in the multitenant cloud environment the confidentiality of data gets compromised because of its misuse, and this is where these threats come into elaborate activities like unauthorized access, interception of data, and uncontrolled share. Whereas there should be enforcement of mechanisms to ensure data confidentiality and governance.

B. Key Management

Keeping key management in place is the most severe challenge to the protection of encrypted cloud data. Keys that get stolen or compromised pose a risk for data loss. Large key sizes are therefore required to avoid unauthorized decryption.

C. Vendor Lock-in

Cloud providers restrict user flexibility through lock-in periods, preventing seamless migration to alternative service providers despite customer dissatisfaction [20].

D. Anomaly Detection

Anomaly detection mechanisms identify atypical cloud network movements through various detection strategies combined with safety procedures for stored data protection [21].

E. Service Abuse and Identity Management

Attacks can be made by breaching access control in order to gain unauthorized services. In de-duplication processes [22], clients may expose hash values that can be put to unauthorized data access [23]. Self-deterministic identity management approaches give rise to new alternatives in a trustless environment [24].

V. Privacy Models and Protection Mechanisms

A. Differential Privacy

Clearly, differential privacy enhances privacy well due to strong privacy guarantees. Here the presence or absence of a user in the dataset must not affect the analysis outcome appreciably. A particular perturbation of the data associated with counting of the attributes gives differential privacy [25].

Experimental results show that the proposed algorithms for differential privacy achieve significantly lower MAE and MRE compared to the benchmark algorithms. For Count queries with $\alpha = 0.5$ and a query size of 3, the proposed algorithm has an MAE of less than 20, while the benchmark shows an MAE nearing 70. For Sum queries with query size 4 and $\alpha = 0.5$, the proposed algorithm achieves an MRE of less than 0.1 against the benchmark MRE of greater than 0.2 [26].

B. K-Anonymity

K-anonymity is the first syntactic mechanism for cybersecurity, indicating that an anonymized dataset must have at least k records that are grouped equivalently. Now for all k-anonymous data groupings, individual probability of re-identification is equal to 1/k. For k-anonymity, masking procedures are:

Generalization: Matching data are grouped into k-groups by substituting some quasi-identifying fields with shared cluster attributes.

Micro-aggregation: It uses averaging or cluster centroid values to minimize data loss by then aggregating matched records into k-groups and replacing quasi-identifiers.

Local Suppression: It removes some than uncommon property values and replaces locations with missing value, improved quasi-identifier features sharing in records.

C. L-Diversity and T-Closeness

L-Diversity employs the Bayes optimal privacy principles and also eliminates the linkages that the records-attribute pair can make. The l-diversity model fails in practical implementation in cases where the sensitive values include a small number of distinct values as well as classes that are skewed in terms of their membership [27].

T-closeness is an amalgam of l-diversity and k-anonymity principles, which have brought down inconsistencies that occur in case privacy and utility metrics are concerned.

VI. Blockchain-based Access Control

A. Role-Based Access Control (RBAC)

RBAC allows diverse task execution of operations by customers operating with the permission sets P and the associated users U[28]. An all-inclusive framework for operational independence with functional separation, flexible in working.

B. Attribute-Based Access Control (ABAC)

ABAC consists of structural models for information access control standards and approach models showing ABAC characteristics itself. Under ABAC, the three types of attributes are:

Subject Attributes: Member identifiers accessing an asset, employee title, organizational affiliation, and identifier.

Asset Attributes: Properties linked to the resource accessed and augmented, and validating controlling decisions.

Environment Attributes: Contextual characteristics including current time/date, pertinent administrations, and information security phase [29].

C. Blockchain-Based Access Control Implementation

In a decentralized security solution that combines blockchain with entrance regulators, data privacy is guaranteed. This is done by getting approval via the blockchain-based DHTs (distributed hash tables) and pointers for the storage of encoded data [30].The blockchain has two main functions for checking the identity and authorization of the user for the retrieval of data and the generation of encryption keys based on composite characters incorporating the respective login credentials of both the users and assistance systems [31].

VII. Data Protection Framework

This comprehensive system of data protection consists of four different security layers:

- The user layer opens the entry points to the data resource by authenticated and authorized user credentials. The access rights themselves are established by the user layer authentication.
- The communication layer employs cryptography and other classifications so that secure transfer of data is accomplished between the users and the cloud systems.
- The end storage is precisely the first point gathering data and a monitoring mechanism intended to validate the successful implementation of the security policies along the storage pipeline.
- The control layer performs monitoring and validation of the impact of security measures on controlling the operations of the system.

VIII. Results and Discussion

A. Differential Privacy Performance

Experimental validation has shown significant improvements in the proposed differential privacy algorithm's performance against benchmark implementations.

As the size of the dataset progresses from 1,500,000 to 4,500,000 records with an α=0.5, the Sum query relative error drops from 0.7 to below 0.6, hence bringing better data accessibility into large size multi-dimensional datasets [32].

B. Cybersecurity Properties Provision

Study of the application of Blockchain reveals a 67% domination of recent proposals in terms of provision for full authentication compared to what has been achieved from initial offerings (started around 2014) [33]. From the above, it can be observed that the most common method for authentication, especially in many private and permissioned networks, is the registration/enrollment in comparison to previous public permissionless networks, such as Bitcoin.

To put it another way, "Analysis of blockchain implementations reveals an increasing provision of authentication from approximately 67% of recent proposals in complete authentication against initial offering (from 2014) [34]. On the basis of the above, it can be said that registration/enrollment is the favored mode for authentication, especially in most private and permissioned networks in comparison to previous public permissionless networks like Bitcoin."

Hence, the country came up with several collaborations through which it has built a successful federation of almost all its states with the best plans.

In short, this would involve private and permissioned networks, as opposed to previous registrations in public permissionless networks like Bitcoin.

C. Security Technique Evolution

From 2014 through 2015, different methods of authentication were tried out off the chain. In subsequent years, authentication moved into registration/pre-enrollment techniques and come now to a stage where trusted third parties come into use, although there is an increasing preference for completely decentralized approaches to eliminate any single points of failure.

IX. Blockchain-Cloud Integration Benefits

A. Enhanced Security

Blockchain silica bonds integration has secured trust towards automated control security through smart contracts, completely automating the authorization of cloud services, IoT operations, and security risk prevention to the aforementioned cloud resources [35].

B. Improved Privacy

User actions are kept under control by transparent audit trails, which preserve control of device and data and increase informational security with various automated access control mechanisms.

C. Scalability and Performance

Blockchain technology has to be complemented with on-demand processing capabilities, which cloud resources provide.

Such capabilities enable large-scale transaction data processing and allow adapting integrated solutions for the achievement of high-level flexibility.

D. Fault Tolerance

Deprived cloud services by replication make the multi-ported sharing and distribution of all data of the blockchain on all machine systems linked to the environment without a single point of failure and provide continuous service realization, inception, or failure during the attack or component failure.

Data replication in Clouds facilitates the sharing and distribution of data from the blockchain within each connected machine system, hence protecting against a single point of failure while assuring service continuity during an attack or failure of the component.

X. Applications in IoT-Enabled Systems

The Bcot apps are cataloged under different domains. Smart Healthcare covers Patient data management along with the privacy regulation and access control from the smart contracts.

Smart Cities: has distributed resource management and secure IoT device coordination without centralized control.

Smart Transportation: handles the communication between vehicle-infrastructure and transaction records that can be tracked.

Manufacturing processes: It makes a Transparent and secure supply chains through immutable ledger record are the domains of Smart Industries.

XI. Conclusion

This paper looks into security improvement in cloud applications by the blockchain approach through complete analysis of integrated mechanisms, privacy-preserving models, and access control strategies. Findings indicated that basic vulnerabilities of the Cloud of Things have been responded to by integration with decentralization, continuous, and cryptographically protected records, while assured operational scalability via support of cloud resources.

Differential privacy systems perform significantly better in regard to error measures as compared to any other benchmarks in the class. Access control implementations on the blockchain provide better solutions for granularity of security while operating towards minimizing the trust in the third-party agents. BCoT combines the security features of blockchain with those of scalability and fault tolerance from cloud computing.

Future work should perhaps begin focusing on the optimization of real-time consensus mechanisms in large IoT networks and methods for formal verification of smart contracts, among many others. An avenue of many other opportunities will arise in the integration with the cutting-edge technologies of edge computing and quantum-resistant cryptography for next-generation secure cloud infrastructures.

References

[1] G. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Cryptocurrencies and Blockchain, 2008.

[2] V. Ashok, J. Anitha, I. De la Torre Díez, and D. J. Hemanth, “Prediction of epileptic seizure using deep learning architectures,” Int. J. Med. Eng. Informat., vol. 17, no. 3, pp. 267–278, 2025, doi: 10.1504/IJMEI.2025.145853.

[3] NIST, "Cloud computing security considerations," National Institute of Standards and Technology Special Publication 800-145, 2011.

[4] A. Vajravelu, Y. Thanikachalam, M. H. B. A. Waha, M. M. B. A. Jamil, and S. Sivaranjani, “Human-machine collaboration and emotional intelligence in Industry 5.0,” in Human Machine Collaboration and Emotional Intelligence in Industry 5.0, 2024, pp. 220–232, doi: 10.4018/979-8-3693-6806-0.ch012.

[5] P. Sarvalingam, A. Vajravelu, M. M. B. A. Jamil, S. R. Ahammed, and J. Selvam, “EEG-based classification for autism spectrum disorder and emotional state recognition—A critical evaluation,” in Proc. 2024 4th Int. Conf. Ubiquitous Comput. Intell. Inf. Syst. (ICUIS), Dec. 2024, pp. 1935–1941, doi: 10.1109/ICUIS64676.2024.10866715.

[6] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," in Proceedings of the 16th International Conference on Distributed Computing and Networking, 2015, pp. 1–6.

[7] V. Ashok and G. Murugesan, “Detection of retinal area from scanning laser ophthalmoscope images (SLO) using deep neural network,” Int. J. Biomed. Eng. Technol., vol. 23, no. 2–4, pp. 303–314, 2017, doi: 10.1504/IJBET.2017.082668.

[8] V. Ashok and K. S. Tamilselvan, “Determination of blood constituents using laser based systems,” Asian J. Inf. Technol., vol. 15, no. 21, pp. 4299–4301, 2016, doi: 10.36478/ajit.2016.4299.4301.

[9] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 464–469.

[10] V. Ashok, A. Nirmalkumar, J. Shanthi, and S. R. Singh, “A non-invasive empirical approach of human blood and tissues through laser trans-illumination and back scattering profiles,” Eur. J. Sci. Res., vol. 47, no. 1, pp. 107–117, 2010.

[11] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[12] M. R. Bhaskar, "Cloud computing service models," International Journal of Cloud Computing and Services, vol. 4, no. 2, pp. 112–128, 2018.
[13] K. Hariraman, J. Selvam, M. Alagirisamy, and S. S. Sivaraju, “An improved carbon cloth structure for asymmetric supercapacitor design,” in Proc. 2022 4th Int. Conf. Inventive Res. Comput. Appl. (ICIRCA), Sep. 2022, pp. 48–56, doi: 10.1109/ICIRCA54612.2022.9985646.
[14] A. Markandey, "Software as a Service (SaaS) in enterprise computing," Journal of Information Technology Management, vol. 15, no. 3, pp. 45–62, 2019.
[15] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST Special Publication 800-144, 2011.
[16] Y. M. Thu and J. Selvam, “Pre-stress linear and nonlinear buckling of cold-formed steel built-up box studs,” Int. J. Sustain. Constr. Eng. Technol., vol. 14, no. 2, pp. 114–120, 2023, doi: 10.30880/ijscet.2023.14.02.012.
[17] L. K. Garrison, "Private cloud infrastructure assessment," IEEE Transactions on Cloud Computing, vol. 3, no. 1, pp. 78–91, 2016.
[18] N. Sultan and I. Weill, "Information systems outsourcing: A survey and analysis of the literature," ACM SIGMIS Database for Advances in Information Systems, vol. 36, no. 4, pp. 23–58, 2005.
[19] O. P. Giri, P. B. Shahi, J. Selvam, S. Poddar, and A. Bhaumik, “Road traffic regulation and enforcement status: A Nepalese traffic police perspective,” Transp. Res. Interdiscip. Perspect., vol. 26, p. 101188, 2024, doi: 10.1016/j.trip.2024.101188.
[20] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing—The business perspective," Decision Support Systems, vol. 51, no. 1, pp. 176–189, 2011.
[21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," whitepaper, 2008.
[22] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2016 IEEE 6th International Conference on Big Data Computing Service and Applications (BigDataService), 2016, pp. 459–464.
[23] Y. Saleh and K. Hock, "Blockchain-based smart contracts: A systematic mapping study," in Proceedings of the International Workshop on Requirements Engineering for Blockchain, 2018, pp. 11–18.
[24] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[25] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2017, pp. 2567–2572.
[26] M. Swan, Blockchain: Blueprint for a new economy. O'Reilly Media, 2015.
[27] V. Buterin et al., "A next-generation smart contract and decentralized application platform," Ethereum Whitepaper, 2014.
[28] C. Kaufman, R. Perlman, and M. Speciner, Network security: Private communication in a public world. Prentice Hall Press, 2002.
[29] A. Shamim and M. Ahmed, "Cloud data security using encryption and access control," International Journal of Cloud Computing, vol. 5, no. 2, pp. 134–150, 2020.
[30] C. Manonmani, A. Vajravelu, S. Vidhya, and S. Degadwala, "Design and Implementation of Self-Powered Reconfigurable Intelligent Surfaces: Applications and Future Trends," in Applications and Challenges of Reconfigurable Intelligent Surfaces in 6G, 2025, pp. 379–407, doi: 10.4018/979-8-3693-8099-4.ch015.
[31] S. Seenuvasamurthi, S. Ashok, B. Shankarlal, A. M. Abbas, and A. Vajravelu, "Brain Image Compression and Reconstruction System Using Deep Learning," International Journal of Medical Engineering and Informatics, vol. 16, no. 5, pp. 401–413, 2024, doi: 10.1504/IJMEI.2024.140799.
[32] R. Rajaram, M. Midhunchakkaravarthy, J. Selvam, and A. Vajravelu, "Enhancing Lung Cancer Detection Using VGG-16: Leveraging Deep Convolutional Neural Networks for Accurate Medical Image Analysis," in Proc. 2024 2nd International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), 2024, pp. 190–194, doi: 10.1109/ICMACC62921.2024.10894308.
[33] K. Sravanthi, V. Valikar, S. Sri Nandhini Kowsalya, A. Mutharasan, and A. Vajravelu, "Federated Learning-Based Energy Management Systems for Privacy-Preserving Demand Forecasting in Smart Cities," in Proc. 13th IEEE International Conference on Smart Grid (ICSMARTGRID), 2025, pp. 446–451, doi: 10.1109/ICSMARTGRID66138.2025.11071727.
[34] V. Ashok, A. Nirmalkumar, and N. Jeyashanthi, "A Novel Method for Blood Glucose Measurement by Noninvasive Technique Using Laser," World Academy of Science, Engineering and Technology, vol. 51, pp. 676–682, 2011.
[35] V. Ashok, A. Nirmalkumar, J. Shanthi, and S. R. Singh, "A Non-Invasive Empirical Approach of Human Blood and Tissues Through Laser Trans-Illumination and Back Scattering Profiles," European Journal of Scientific Research, vol. 47, no. 1, pp. 107–117, 2010.