EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Blockchain based Quantum Resistant Signature Algorithm for Data Integrity Verification in Cloud and Internet of Everything

Pranav Shrivastava[1,*], Bashir Alam[2], Mansaf Alam[3]

[1,2] Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India
[3] Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Abstract

INTRODUCTION: The processing and storage capacities of the Internet of Everything (IoE) platform are restricted, but the cloud can readily provide efficient computing resources and scalable storage. The Internet of Everything (IoE) has expanded its capabilities recently by employing cloud resources in multiple ways. Cloud service providers (CSP) offer storage resources where extra data can be stored. These methods can be used to store user data over the CSP while maintaining data integrity and security. The secure storage of data is jeopardized by concerns like malicious system damage, even though the CSP's storage devices are highly centralized. Substantial security advancements have been made recently as a result of using blockchain technology to protect data transported to networks. In addition, the system's inclusive efficacy is enhanced, which lowers costs in comparison to earlier systems.
OBJECTIVES: The main objective of the study is to a blockchain-based data integrity verification scheme is presented to provide greater scalability and utilization of cloud resources while preventing data from entering the cloud from being corrupted.
METHODS: In this paper, we propose a novel method of implementing blockchain in order to enhance the security of data stores in cloud.
RESULTS: The simulations indicate that the proposed approach is more effective in terms of data security and data integrity. Furthermore, the comparative investigation demonstrated that the purported methodology is far more effective and competent than prevailing methodologies.
CONCLUSIONS: The model evaluations demonstrated that the proposed approach is quite effective in data security.

Keywords: Data integrity verification, blind signature algorithm, lattice cryptography, puzzle optimization algorithm, blockchain, upgraded Merkle tree, vacuum filter, quantum resistant

Received on 20 December 2023, accepted on 14 March 2024, published on 20 March 2024

doi: 10.4108/eetsis.5488

*Corresponding author. Email: pranav.paddy@gmail.com

1. Introduction

Cloud computing has grown in popularity as a result of the outsourcing of processing and the rendering of storage requirements depending on user availability. On the basis of shared services, users can access resources such as applications, services, bandwidth, and storage via the internet [1]. The essential aspect of cloud computing is the centralized outsourcing of user data, with the CSP acting as a resource provider. The Internet of Everything (IoE) is a concept whose architecture and environment include components of the Internet of Things (IoT) [2][3]. People, Data, and Processes are the other three aspects in an IoE scenario. Data collection is an important aspect of IoE [4]. Every day, additional data is collected in the IoE context. These applications make use of low-performance, low-power-consumption components that are incapable of providing considerable processing capability to the architecture.

Blockchain technology is already emerging as a very important frontier field in the case of cutting-edge value theories and diverse application scenarios due to its specific technological advantages [5][6]. Blockchain functions as a distributed database composed of blocks, smart contracts, transactions, consensus processes, and so on. Every block's header field includes the previous block's hash value, resulting in an ordered chain [7]. The primary benefits of blockchain technology are the creation of an open, decentralized, auditable, transparent, and tamper-proof record. Every blockchain node may validate the transactions that have been logged on the chain. Because the transactions are enduringly chronicled on the blockchain, the data cannot be deliberately updated. Every document has an irreversible and permanent time stamp [8][9]. Because blockchain technology shatters the centralized elements of the internet, greater security may be provided.

Once the transaction is performed and authenticated, the participants can have a high level of trust in the blockchain [10]. Blockchain can help to tackle the hindrance of data authenticity. It can efficiently endorse data interchange and circulation [11]. Data integrity is the guarantee that the stored information is undamaged and may only be viewed or updated by the appropriate individuals [12]. As a result, developing an effective blockchain system is critical for promoting data integrity.

The paper is discussed along these lines: in Section 2 the literature review of the prevailing techniques is presented, under Section 3 the propositioned methodology with algorithms and descriptions are provided, under Section 4 outcomes and analysis are demonstrated and Section 5 concludes the paper with future scopes.

2. Literature Review

The literature review explores the integration of blockchain technology and quantum-resistant signature algorithms for ensuring data integrity in Cloud and Internet of Things (IoT) environments. By analyzing existing research and developments, this review aims to elucidate the current state-of-the-art techniques, challenges, and future prospects in this burgeoning field. Addressing the critical need for secure data management in increasingly interconnected systems, the review highlights the potential of these innovative approaches.

Sim et al. [13] proposed an IoT data integrity verification based on blockchain for enhancing IoT edge computing environment. To reduce IoT data redundancy, the suggested method combines signature and data keys from various IoT devices housed in grouped subsets in the IoT edge computing environment, building many hash chains utilizing blockchain technology.

Xie et al. [14] proposed an effective blockchain-based solution for data integrity verification in cloud environment. By solving a few limitations of traditional centralized auditing and enhancing the plan's effectiveness and security through usage of the blockchain network. In contrast, based on the SIS problem assumption, the system may withstand the threat posed by quantum computing while simultaneously streamlining the user verification procedure, partially alleviating the issue of users' limited computational capability.

Li et al. [15] proposed a secure picture sensing transmission and storage technique for blockchain in the IoT. The blocking procedure for data and image detection of smart image sensors; the algorithms for generating public and private keys for detecting data blocks; and the algorithms for signing and validating signatures for detecting data blocks are the essential components of this solution. However, this method is difficult to utilize and time intensive.

Zhao et al. [16] presented a novel procedure using Merkle tree reconstruction, that enhances some aspects such as fault tolerance and information security when compared to conventional approaches and improves the block generation criteria to make it more appropriate for improve system performance in agricultural IoT data. Nonetheless, this approach demands the use of additional equipment to carry out the information security evaluations.

Bai et al. [17] presented a lightweight BPIIoT to aid in the development of an end-to-end, decentralized industrial applications. The BPIIoT platform is built on a blockchain network that includes smart contracts. The BPIIoT platform is designed to be a light-weight network infrastructure comprised of an on-chain network and an off-chain network to reduce network load and latency. This strategy, however, cannot be used in business settings.

The majority of the strategies studied focused on improving the overall performance of the algorithms by boosting throughput and time. The existing work was missing out on the following parameters, computational feasibility, interoperability and scalability. Furthermore, existing strategies are incapable of providing protection against quantum attacks, which is the primary emphasis of the proposed work. Blockchain has recently been regarded as one of the most effective solutions for security challenges. Because blockchain employs both cryptography and hashing techniques, data security is enhanced, in addition to several other advantages. Though there are a lot of literary works built on blockchain, most of them have one or more performance difficulties. In this study, a blockchain-based architecture is offered as a way to provide a higher level of security and integrity to data transferred to cloud servers.

3. Methodology

Cloud services are popular among customers because they give a variety of computing capabilities as well as flexible storage. Data storage in cloud servers provides numerous benefits, including remote access support, lower hardware investment costs, and reduced local storage strain. Though the cloud has increased the general convenience of storage facilities for its customers, it has also introduced new issues that must be handled quickly. Some of the most prevalent cloud challenges are data corruption, user data security, increased system vulnerability, tampering, and data loss. These obstacles impede the cloud's reputation from spreading to users all around the world. As a result, it is critical to propose some technique or algorithm that may successfully improve data integrity in the cloud. This effort decides to administer blockchain technology for improving the privacy of data stored in the cloud. Furthermore, a blockchain-based data integrity verification scheme is presented to provide greater scalability and utilization of cloud resources while preventing data from entering the cloud from being corrupted. Figure 1 depicts the suggested framework architecturally.

The planned task is divided into six major phases: key generation, signature generation, file upload, audit request, proof generation, and verification. Users generate keys and signatures in the early phase using the lattice founded blind signature algorithm (L_BSA). During the key creation step, the keys are produced at random, and an optimal key is then chosen using the puzzle optimization algorithm (POA). The data is then encrypted and updated using the upgraded Merkle tree aided vacuum filter (Vac-UMT) method with the selected key. The encrypted data is subsequently transformed into blocks and posted to the CSP using blockchain technology. CSP verifies the user's signature whenever he or she sends an audit request for data access. If the user's signature is validated, the cloud server generates an evidence report and sends it to the user for integrity verification. Otherwise, the user's access will be restricted during the evidence generation phase.

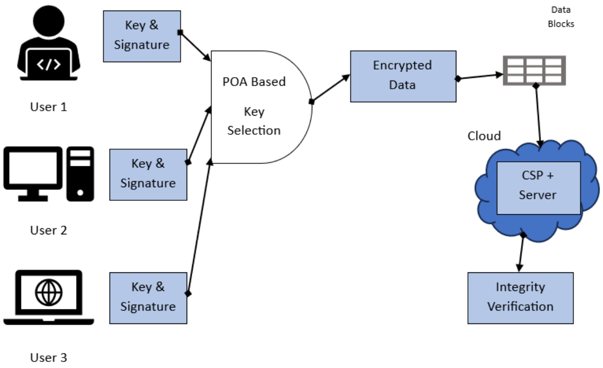

Figure 1: Architecture of the proposed scheme

4. Results

Several experiments and analyses are carried out to demonstrate the suggested method's performance efficacy in comparison to existing blockchain-based data integrity verification systems. The proposed method has been tested in a variety of experimental circumstances, and the results have been thoroughly examined. The implementation scenario, performance measurements concentrated, and analysis performed are all discussed in the following sections.

4.1 Simulation Scenario

Initially, the suggested system produces the key and signatures for user data using the L_BSA technique. The POA algorithm, which is population-based, is then used to select an optimal private and public key, with the initial population set to 300 and the maximum iterations set to 500. The algorithm selects the most optimum key to govern the encryption process based on the fitness evaluation. In this paper, a new and efficient Vac-UMT method for encrypting user data for uploading is provided. The encrypted data is then broken down into blocks before being sent to cloud servers for storage. The audit requests are then submitted to the CSP for verification using user signatures, and the valid ones are routed to the server for evidence report production. Following the submission of the evidence report for integrity verification, the vacuum filter lookup method is utilized to establish whether the data matches the original stored data.

4.1 Performance metrics and analysis

Different performance criteria, such as signature size, signature generation time, proof generation time, verification time, and throughput, are used to evaluate the proposed framework. The framework's performance is also compared to that of other existing methods, including the short signature algorithm (ZSS) [18], BLS [19], RSA algorithm, ECC algorithm, lattice with blind signature [20], lattice signature with cuckoo filter, and lattice signature without cuckoo filter [14]. More examples and descriptions of the comparisons and analysis are provided below. Table 1 compares the implementation of the purported and prevailing methodologies in terms of signature size.

Table 1: Performance comparison for signature size

Signature Size (KB)				
No of blocks	RSA	ECC	Lattice with blind signature	Proposed
100	1.81	0.39	57.66	96

200	8.47	0.58	58.45	96
300	17.86	0.76	58.94	87.75

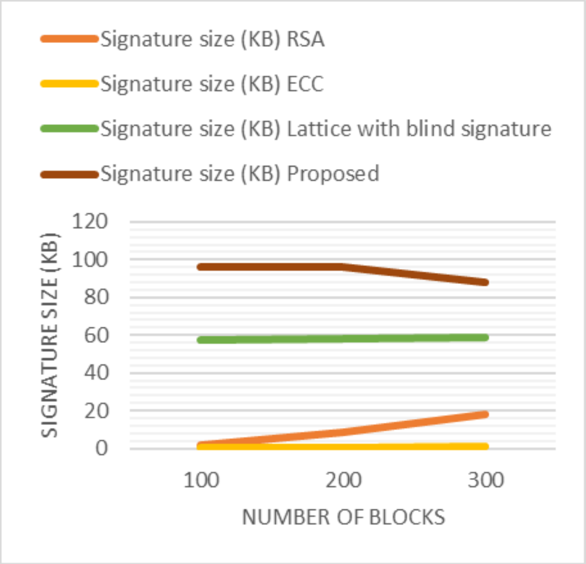

Figure 2: Graphical comparison of signature size

The table values show that the proposed approach produced larger signatures with various levels of security than the other approaches. Figure 2 depicts the graphical representation of the comparison. With increasing security level, the signature size of the RSA algorithm increases, whereas the blind signature scheme only displays a small increase. The suggested scheme's signature size is proven to be more stable as security levels increase. Another significant advantage of the proposed architecture is its ability to withstand quantum attacks, demonstrating its security and utility.

Table 2: Performance comparison for signature generation time

Signature Generation Time (s)				
No of blocks	Lattice signature	ZSS	BLS	Proposed
100	0.45	0.78	2.3	0.032
200	0.78	1.4	4.28	0.065
300	1.08	2.02	6.37	0.099

Table 2 compares the implementation of the purported and existing methodologies in terms of signature creation time. It clearly shows that the proposed strategy is more effective and has a far shorter signature time than the other approaches. Figure 3 depicts a more detailed representation of the signature generation time. The plot was created by randomly arranging 100 to 300 blocks. The proposed approach's signature creation time increases just somewhat as the number of data blocks increases. The signature generation time of the BLS signature is the longest of the compared approaches, while the lattice signature scheme is the shortest. The total analysis shows that the suggested approach is preferable in terms of efficiently producing signatures.

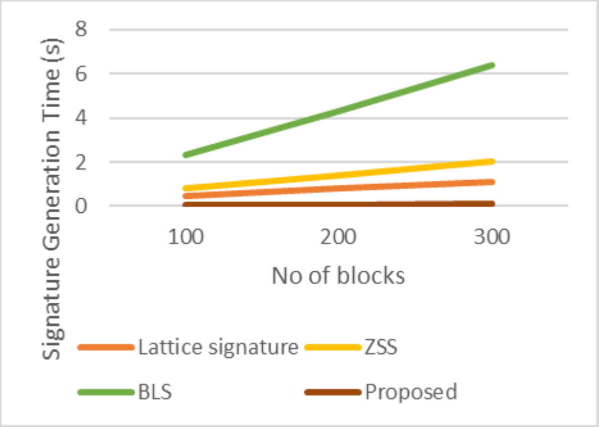

Figure 3: Graphical comparison of signature generation time

Table 3: Performance comparison for proof generation time

Proof Generation Time (s)				
No of blocks	Lattice signature	ZSS	BLS	Proposed
100	0.17	0.35	0.33	0.02
200	0.32	0.56	0.5	0.036
300	0.46	0.83	0.64	0.05

Table 3 compares the implementation of the purported and existing methods in terms of proof generating time. Based on the values, it is obvious that the suggested strategy takes less time to generate proofs than the other approaches. This is also more easily seen in the graphical form shown in Figure 4. The proposed method shows just a minimal increase in time as the number of data blocks increases. The comparative methods resulted in longer proof creation times, which is inefficient. The proposed approach takes only 0.05 s to complete 300 blocks, indicating that the system is highly efficient.

Table 4 compares the implementation of the purported and existing methodologies in terms of verification time. The values show that the proposed approach takes substantially less time to complete the verification process than the other approaches. This is also better represented in Figure 5's graphical portrayal. The proposed solution is clearly indicated in the graphic as being more optimal than the other methods. Furthermore, the BLS signature approach required more verification time, whereas the lattice signature with cuckoo filter method produced comparable results to the suggested method.

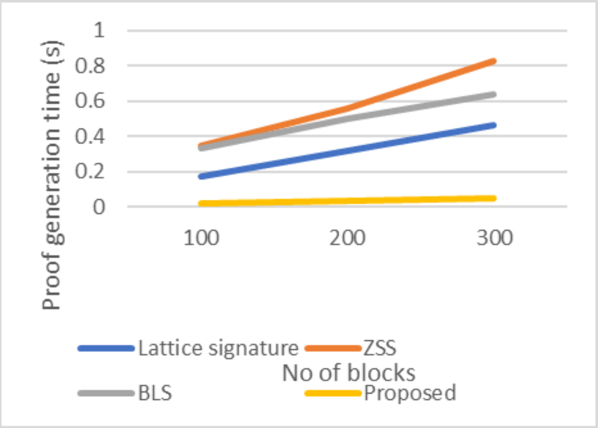

Figure 4: Graphical comparison of proof generation time

Table 4: Performance comparison for verification time

Verification Time (s)				
No of blocks	ZSS	BLS	Lattice signature with cuckoo filter	Proposed
100	7.81	187.49	164.06	2.234
200	8.67	254.75	317.26	3.749
300	9.56	325.94	470.47	5.08

Overall, the simulations indicate that the proposed approach is more effective in terms of data security and data integrity. Furthermore, the comparative investigation demonstrated that the purported methodology is far more effective and competent than prevailing methodologies. The suggested method takes essentially no time to complete the signature generation, proof generation, and verification operations in comparison to existing methodologies. Furthermore, the proposed technique may withstand quantum attacks, which will be advantageous in the future. The advent of quantum computers may cause various security challenges throughout the network, and the most important one will be the implementation of an effective and efficient security model. To meet these objectives, the proposed model, which is very practical and efficient, is introduced. In addition, the research shows that the purported strategy takes substantially less time to verify than the other methods. Furthermore, the total throughput of the suggested technique is quite high, with just a slight loss in throughput as node sizes are raised. Overall, it is demonstrated that the proposed strategy is more ideal and may provide a higher level of security and integrity to data uploaded to the cloud.

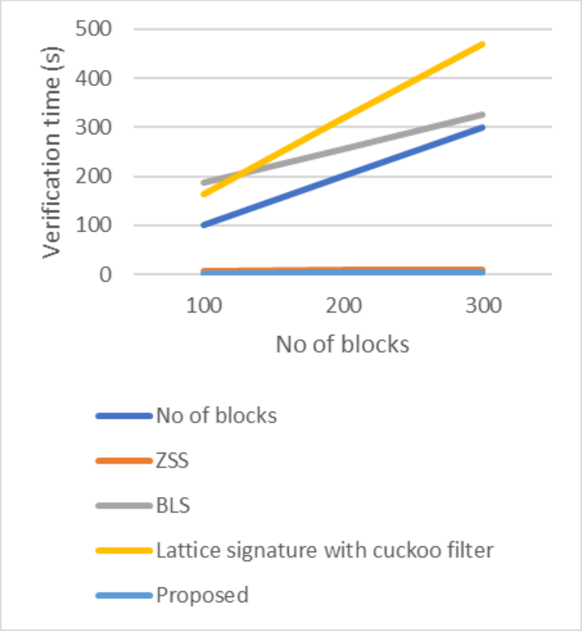

Figure 5: Graphical comparison of verification time

5. Conclusion

The cloud computing ecosystem has several machines that are occasionally hacked by attackers, resulting in data tampering difficulties. Using blockchain technology, this paper aims to improve the security and integrity of data transferred to the cloud. It is critical to protect the files that users upload by not allowing any tampering or data alterations. The proposed blockchain-based infrastructure ensured improved data security and integrity. The complete architecture is simulated in JAVA and tested on the publicly available UNSW-NB15 dataset. The model evaluations demonstrated that the proposed approach is quite effective in data security. Despite its security, the suggested framework is also highly efficient and can finish the verification procedures in a short period of time. In the future, the suggested approach will be tested in real-time cloud environments with larger and more complicated datasets, such as big data.

References

[1] Neela, K. L., and V. Kavitha. "An improved RSA technique with efficient data integrity verification for outsourcing database in cloud." Wireless Personal Communications 123, no. 3 (2022): 2431-2448.

[2] Mohanty, Saraju P., Venkata P. Yanambaka, Elias Kougianos, and Deepak Puthal. "PUFchain: A

hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)." IEEE Consumer Electronics Magazine 9, no. 2 (2020): 8-16.

[3] Mohanty, Saraju P. "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era." IEEE Consumer Electron. Mag. 9, no. 2 (2020): 4-5.

[4] Sun, Yi, Shiqing Jiang, Wanjiao Jia, and Yu Wang. "Blockchain as a cutting-edge technology impacting business: A systematic literature review perspective." Telecommunications Policy 46, no. 10 (2022): 102443.

[5] Nanda, Ipseeta, Lizina Khatua, N. Rajendran, Arun Kumar Marandi, C. R. Manjunath, and M. Sathish. "Security Analysis Using Blockchain Based Key Aggregation Cryptosystem with Time Complexity Reduction." International Journal of Intelligent Systems and Applications in Engineering 10, no. 3s (2022): 133-137.

[6] Nabila, Efa Ayu, Sugeng Santoso, Yudi Muhtadi, and Budi Tjahjono. "Artificial intelligence robots and revolutionizing society in terms of technology, innovation, work and power." IAIC Transactions on Sustainable Digital Innovation (ITSDI) 3, no. 1 (2021): 46-52.

[7] Chen, Lanxiang, Qingxiao Fu, Yi Mu, Lingfang Zeng, Fatemeh Rezaeibagha, and Min-Shiang Hwang. "Blockchain-based random auditor committee for integrity verification." Future Generation Computer Systems 131 (2022): 183-193.

[8] Wu, Wei, Yelin Fu, Zicheng Wang, Xinlai Liu, Yuxiang Niu, Bing Li, and George Q. Huang. "Consortium blockchain-enabled smart ESG reporting platform with token-based incentives for corporate crowdsensing." Computers & Industrial Engineering 172 (2022): 108456.

[9] Manda, Vijaya Kittu, and Satya Yamijala. "Peer-to-peer lending using blockchain." International Journal Of Advance Research And Innovative Ideas In Education 6 (2019): 61-66.

[10] Shrivastava, P., Alam, B. & Alam, M. Security enhancement using blockchain based modified infinite chaotic elliptic cryptography in cloud. Cluster Computing (2022). https://doi.org/10.1007/s10586-022-03777-y

[11] Mohanta, Bhabendu Kumar, Debasish Jena, Somula Ramasubbareddy, Mahmoud Daneshmand, and Amir H. Gandomi. "Addressing security and privacy issues of IoT using blockchain technology." IEEE Internet of Things Journal 8, no. 2 (2020): 881-888.

[12] Wei, Peng Cheng, Dahu Wang, Yu Zhao, Sumarga Kumar Sah Tyagi, and Neeraj Kumar. "Blockchain data-based cloud data integrity protection mechanism." Future Generation Computer Systems 102 (2020): 902-911.

[13] Sim, Sung-Ho, and Yoon-Su Jeong. "Multi-blockchain-based IoT data processing techniques to ensure the integrity of IoT data in AIoT edge computing environments." Sensors 21, no. 10 (2021): 3515.

[14] Xie, Gaopeng, Yuling Liu, Guojiang Xin, and Qiuwei Yang. "Blockchain-based cloud data integrity verification scheme with high efficiency." Security and Communication Networks 2021 (2021): 1-15.

[15] Li, Yunfa, Yifei Tu, Jiawa Lu, and Yunchao Wang. "A security transmission and storage solution about sensing image for blockchain in the Internet of Things." Sensors 20, no. 3 (2020): 916.

[16] Zhao, Yingding, Qiude Li, Wenlong Yi, and Huanliang Xiong. "Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain." Agriculture 13, no. 2 (2023): 274.

[17] Bai, Li, Mi Hu, Min Liu, and Jingwei Wang. "BPIIoT: A light-weighted blockchain-based platform for industrial IoT." IEEE Access 7 (2019): 58381-58393.

[18] Zhu, Hongliang, Ying Yuan, Yuling Chen, Yaxing Zha, Wanying Xi, Bin Jia, and Yang Xin. "A secure and efficient data integrity verification scheme for cloud-IoT based on short signature." IEEE Access 7 (2019): 90036-90044.

[19] Wang, Cong, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for secure cloud storage." IEEE transactions on computers 62, no. 2 (2011): 362-375.

[20] Li, Chaoyang, Yuan Tian, Xiubo Chen, and Jian Li. "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems." Information Sciences 546 (2021): 253-264.