Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 2103–2114
DOI : 10.47974/JDMSC-2368

An enterprise blockchain model : A reliable cryptography-based cyber-physical systems for securing user data

V. Ramachandran *
Department of Computer Science and Engineering
GITAM School of Computing
GITAM Deemed to be University
Bengaluru 561203
Karnataka
India

Hayder M. A. Ghanimi †
Department of Information Technology
College of Science
University of Warith Al-Anbiyaa
Karbala 5751
Iraq

and

Department of Computer Science
College of Computer Science and Information Technology
University of Kerbala
Karbala 5751
Iraq

Bhaskar Marapelli §
Department of Computer Science & Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram 522302
Andhra Pradesh
India

* *E-mail:* ramachandran.veer@gmail.com (Corresponding Author)
† *E-mail:* hayder.alghanami@uowa.edu.iq
§ *E-mail:* bhaskarmarapelli@gmail.com

Navleen Kaur [‡]
Department of Finance
Amity International Business School
Amity University
Noida 201313
Uttar Pradesh
India

M. Rajya Laxmi [@]
School of Business
SR University
Warangal 506371
Telangana
India

Ravi Kumar Bommisetti [#]
Department of Commerce
Akal University
Talwandi Sabo
Bathinda 151302
Punjab
India

Sudhakar Sengan [$]
Department of Computer Science and Engineering
PSN College of Engineering and Technology
Tirunelveli 627152
Tamil Nadu
India

Pankaj Dadheech [^]
Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India

Abstract

This paper introduces a Cyber-Physical System (CPS) that can be used to improve privacy protection in enterprise Blockchain (BC) systems, particularly in Hyperledger Fabric

[‡] *E-mail:* **drnavleenk@gmail.com**
[@] *E-mail:* **laxmi.gunna@gmail.com**
[#] *E-mail:* **ravi9949418650@yahoo.com**
[$] *E-mail:* **sudhasengan@gmail.com**
[^] *E-mail:* **pankajdadheech777@gmail.com**

(HF). The proposed CPS employs advanced methods to facilitate a privacy-preserving authorization mechanism. Using data masking, Homomorphic Encryption (HE), and complex digital signatures, the model ensures the confidentiality of transaction data during the authorization process. Additionally, the implementation of Secure Multiparty Computation (SMC) and Zero-Knowledge Proofs (ZKP) enhances the security of the data by preventing unauthorized personnel from accessing it and ensuring that the approving peers remain anonymous. The solution proposed in the paper addresses the problems of conventional centralized access control, which can be manipulated and has data leakage problems. Experimental results have proved the design's practical applicability and security trade-off, providing a robust foundation for enterprises to adopt privacy-preserving BC. Thus, the HF platform integration demonstrates the model's real-world applicability, which developed a secure, scalable, and efficient solution for handling sensitive transactions in distributed networks.

Subject Classification: *93E10, 94A13.*

Keywords: *Privacy preservation, Enterprise blockchain, Hyper ledger fabric, Integrity, Data confidentiality.*

1. Introduction

Blockchain (BC) is an information-sharing platform that utilizes an immutable, transparent, and distributed ledger for storing transactions across a network of mutually untrusted nodes [1]. Being absolute, network users can only append data into the ledger without deleting or modifying the existing data. With transparency, entities can maintain a consistent view of every transaction, ensuring non-repudiation of transactions. The distributed nature provides high availability of the shared ledger to all network users [2]. It disregards the requirement for any intermediate trusted entity and allows direct communication between the users, thus transforming any need for trust into a source [3]. Hyperledger Fabric (HF) is an enterprise-grade permissioned BC with an extensible and modular network. It is an open-source platform hosted by the Linux Foundation. It is the first to support Smart Contracts (SC), which is written in a general-purpose programming language such as *Node.js*, Go, and Java, in contrast to other platforms that only have domain-specific language. The permission nature is understood using a membership service provider that provides cryptographic identities to network users for authentication and authorization. Being a grouping BC platform, the users are known in advance but are still untrusted (challengers in an industry) [4]. Moreover, no built-in cryptocurrency makes it suitable for many business applications. With no cryptocurrency, the attack surface is reduced, and no additional

cost is experienced for mining operations. Depending on the application and trust model, it provides a pluggable consensus mechanism (Byzantine Fault-Tolerant (BFT)/Crash Fault-Tolerant (CFT)). Apart from the industry-level identity management system, it provides several privacy and confidentiality features through advanced cryptographic primitives. The Fabric has a maximum Network Throughput (NT) of 20,000 transactions per second with an End-to-End Delay (EED) of 12.36 *ms*, scaling over 100 peers. The advanced Cyber-Physical Systems (CPS) of the Fabric network make it an extensible model as it adapts to changing requirements and improvements. This stands in contrast to an integrated network, where a small change affects the entire CPS due to the absence of distinct modules. As HF is a modular network, it is required to recognize the several components of the network and the communication between the nodes. The fundamental concept of the Fabric model makes it more accessible to identify and address existing faults in the Fabric design and propose viable solutions. The CPS, with its unique transaction flow and privacy features, is provided in HF [5]. Cloud computing (CC) delivers computing services, including servers, storage, applications, databases, networking, and analytics, where computing resources are provided to multiple users and self-managed NT on the internet. However, the concept of cloud security is centralized, and it has problems like alteration and data theft. To address these challenges, the researcher presents AuthPrivacyChain, a BC-based access control framework that maps each BC node address as an identity and encrypts access permissions. As used on the Enterprise Operation System (EOS), AuthPrivacyChain secures against unauthorized access and preserves privacy [6]. Unlike the ordinary Internet of Things (IoT), privacy protection is a significantly larger concern in the Internet of Medical Things (IoMT) due to the sensitive nature of the data involved. Centralized privacy methods are not immune to failures and breaches, which is a significant problem. These problems are resolved by SecureMed NT's distributed authentication of users at NT BC edge cloudlets. It utilizes SC and edge nodes for public/private key authentication and is more efficient in terms of EED, bandwidth, and scalability than traditional methods. Off-chain blockchain Systems (OCBS) are systems that help control data on the blockchain network, thereby increasing scalability and privacy, and minimizing storage requirements. This method is significant in handling healthcare data, as it raises regulatory and privacy concerns. The proposed modular hybrid privacy-preserving framework is designed to capture OCBS features more effectively, in line with the requirements of healthcare data authorities [7, 8]. In human resource management, BC

presents a distributed ledger record-keeping system that is transparent and privacy-preserving. This method involves applying a public-private key pair and SC, and the performance indicators will reveal the efficiency of data Confidentiality, Integrity, and Availability (CAI). Current cloud security solutions often employ centralized access control, which exposes highly confidential data to risks, including breaches. The complication methods used in the privacy-preserving authorization system for HF address this problem by decentralizing access control through the use of encryption and secure multiparty computation, thereby improving data integrity and security against potential hacker intrusions [9-10]. The remainder of the article is organized as follows: the proposed methodology is given in Section 2, the simulation is analyzed in Section 3, and the article is concluded in Section 4.

2. Proposed Methodology – An Effective Cryptographic Model for Privacy Preservation

This section describes the privacy-preserving authorization method in HF by introducing a network comprising several peers, users, and orders. The model of HF can be easily tuned so that peer components are responsible for storing the ledger, users are responsible for initiating positive transactions, and orders must deal with consensus and transaction ordering [11-14]. The SC/BC code is deployed on the users to carry the business logic for validating the transactions. It guarantees that every transaction will be checked and passed NT the authorization policy before it is written on the ledger [15]. Consider an HF with a set of peers $P=\{P_1, P_2,\ldots, P_m\}$, where m is the sum of peers, and a subset $E=\{E_1, E_2,\ldots, E_n\}\subseteq P$ represents the users. The BC code C is a function $C: T\rightarrow$R, where **T** is the transaction input, and **R** is the transaction result Eq. (1).

$$C(T) = R \tag{1}$$

Where T→is the transaction submitted by the client and RRR→is the transaction result after processing by the BC code **C** on the user nodes. Data masking is represented by a function M: D→D′, where D is the original transaction data and D′ is the masked data Eq. (2).

$$D' = M(D) \tag{2}$$

To maintain privacy during the authorization process, data masking is employed. The most crucial part of data masking involves modifying or concealing specific data from users in a transaction. Depending on the

privacy needs of the data, it can be either reversible or irreversible. Homomorphic Encryption (HE) takes privacy to the next level by allowing computations to be performed on encrypted data, thereby ensuring that users of a specified transaction can verify the authenticity of the transaction without ever having to access the plain, unencrypted value. Other forms of signatures, such as ring or group signatures, are used to conceal the identity of users while, at the same time, the network is capable of verifying the users. Secure Multiparty Computation (SMC) distributes the transaction validation computation among users, preventing any single entity from obtaining a complete view of the data, thereby enhancing privacy. HE allows operations on encrypted data. Let E→the encryption function; ⊕→HE corresponding to the operation ⊕ on plain data given in Eq. (3).

$$E(D_1) \oplus E(D_2) = E(D_1 \oplus D_2) \tag{3}$$

Complicated signatures by Eq. (4).

$$\sigma' = O(\sigma, k) \tag{4}$$

Where σ→the original signature; O→the confusion function;k→a key. In SMC, data 'D' is divided into shares '$D_{i'}$ such that 'D'and each user '$E_{i'}$ methods its share (5).

$$D = \sum_{i=1}^{n} D_i \tag{5}$$

The selection of a user 'E_i' can be modeled as a probabilistic function $P(E_{i)=pi}$, where p_i→the probability of selecting 'E_i', Eq. (6).

$$p_i = \frac{1}{n} \text{(For Randomized Selection)} \tag{6}$$

ZKP enables a prover to convince a verifier that a statement is true without revealing the data 'D' itself is assumed in Eq. (7). Let P→the proof function; V→the verification function.

$$V(P(D)) = True \tag{7}$$

The transaction 'T' is submitted to the user in error. Let $T'=O(T)$ be the confused transaction, Eq. (8).

$$T' = O(T) \tag{8}$$

Each user, as Ei , validates the complicated transaction T′ and produces an authorization Ri, as shown in Eq. (9).

$$R_i = C(T') \tag{9}$$

The collected authorizations are ordered and committed as a block 'B', Eq. (10).

$$B = O(R_1, R_2, \ldots\ldots, R_n) \tag{10}$$

Peers verify the block 'B' and the associated signatures σ′ using ZKP, Eq. (11).

$$V(B, \sigma') = True \tag{11}$$

In the privacy-preserving consensus mechanism, user selection is dynamic and can be based on random selection or features. This unpredictability prevents the selection of users from being easily controlled, thus increasing the network's security. Users can utilize ZKP in the consensus process to prove their authorizations are correct while trusting the primary data and maintaining their identity concealed. Using ZKPs, the system preserves the privacy of transaction data and user identities while ensuring the authenticity of authorizations. The first step of the transaction flow involves the client providing a transaction proposal to the approving peers, which is typically encrypted. Users verify the transaction by working with the masked data, which is achieved through methods like HE/SMC, allowing them to validate these transactions without decrypting the sensitive data. After all the required authorizations have been collected, they are sent to the ordering service, which organizes them into blocks to be transmitted among the network's peers. Finally, the peers ensure the integrity of the transaction and the validity of the complicated signatures by using ZKPs, simultaneously preserving the anonymity of the users along with the transaction data.

3. Result and Discussion

The simulation setup requires specific hardware and software configurations. The hardware includes an 8-core CPU, 32 GB of RAM, 1 TB SSD storage, Gigabit Ethernet for networking, and an NVIDIA Tesla GPU for accelerating cryptographic operations. The software environment consists of Ubuntu 20.04 LTS as the operating system, Hyperledger Fabric 2.x as the BC platform, Docker 20.x with Docker Compose for containerization, and Go 1.16+ along with Node.js 14.x for programming. OpenSSL and PyCryptodome are also needed for cryptographic operations, while development and simulation are directed using VS

Code, HF-SDK, Pythereum, and Hyperledger Caliper. The performance of the proposed CPS is evaluated using transaction EED and NT. The performance of the proposed model is compared with that of existing methods, including AuthPrivacyChain, SecureMed, and OBCS. Transaction End-To-End Delay (EED) is the time it takes for a transaction to go through all these steps before being recorded in the BC ledger. This metric assesses the effectiveness of the cryptographic model and the performance of the authorization process, evaluating the time required to complete transactions and authorizations. Network Throughput (NT) is the ratio of the rate at which transactions are completed to the amount of time taken, commonly in TPS, for transactions per second. This measure assesses the CSM and BC's ability to process multiple transactions efficiently, as shown in Equations (12) and (13).

$$Transaction_{EED} = Timestamp_{completion} - Timestamp_{initiation} \tag{12}$$

$$Throughput = \frac{Number\ of\ Transactions}{Time\ Interval} \tag{13}$$

Table 1

Comparison of Transaction EED

Transaction Count	AuthPrivacyChain	SecureMed	OBCS	Proposed CPS
100	67.87	69.78	71.11	50.22
200	68.91	69.9	72.34	51.98
300	69.99	70.91	73.33	53.01
400	70.21	71.23	74.12	54.88
500	71.87	72.23	75.12	55.89

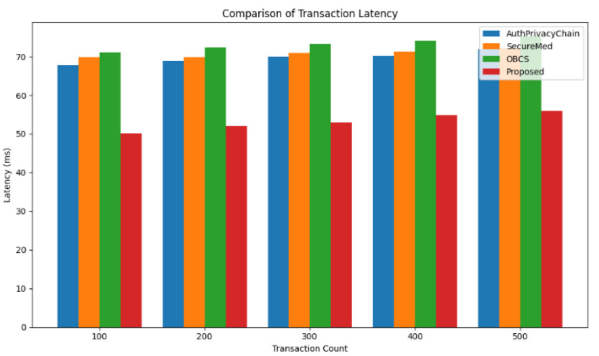

Figure 1

Comparison of Transaction EED

Table 2

Comparison of NT

Transaction Count	AuthPrivacyChain	SecureMed	OBCS	Proposed CPS
100	23.12	19.87	18.67	31.23
200	24.23	19.9	18.91	32.98
300	25.23	20.01	19.02	33.68
400	26.76	21.23	19.12	34.01
500	27.71	21.45	19.33	36

The transaction EED and NT measured in the different systems shows the overall performance disparity. Table 1 shows that the proposed CPS consistently outperforms AuthPrivacyChain, SecureMed, and OBCS in terms of transaction EED. For instance, with 100 transactions, the proposed CPS achieves an EED of 50.22 *m*s, notably lower than AuthPrivacyChain's 67.87 *ms* and SecureMed's 69.78 *ms*. This trend continues as transaction counts increase, with the proposed CPS maintaining the lowest EED across all transaction counts. In Table 2, the proposed CPS also leads NT, processing 31.23 transactions per second at 100 transactions and increasing to 36 TPS at 500. This surpasses AuthPrivacyChain's 23.12 to 27.71 TPS, SecureMed's 19.87 to 21.45 TPS, and OBCS's 18.67 to 19.33 TPS. Figure 1 and Figure 2 visually confirm these findings, highlighting the proposed CPS's efficiency in EED and NT.

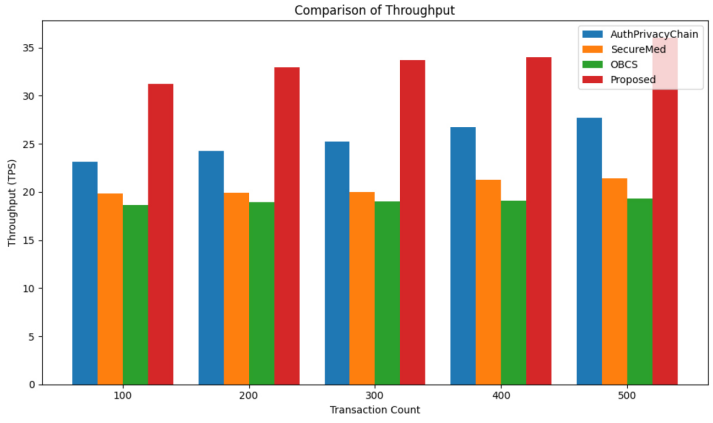

Figure 2

Comparison of NT

4. Conclusion and Future Work

The proposed CPS to preserve privacy in HF can resolve the significant problems related to data security in enterprise BC contexts. Using data masking, HE, confused digital signatures, SMC, and ZKP, the model ensured the privacy and integrity of transactions during the authorization process. The implementation results validate that the proposed CPS can ensure its security, scalability, and efficiency, making it a suitable recommendation for companies seeking to enhance their security based on BC. The recommended model provides strong privacy protection; however, further investigation can be conducted to apply QR-based cryptographic solutions for protection against emerging attacks. Furthermore, fine-tuning the model for large-scale use case scenarios and researching inter-chain compatibility will continue to expand its relevance in the ever-growing and constantly evolving BC.

References

[1] S. Ben Toumia, C. Berger and H. P. Reiser, "An evaluation of blockchain application requirements and their satisfaction in hyper ledger fabric: A practical experience report," In *IFIP International Conference on Distributed Applications and Interoperable Systems*, pp. 3-20, Cham: Springer International Publishing, (2022).

[2] A. A. Dar, F. Reegu and G. Hussain, "Comprehensive Analysis of Enterprise Blockchain: Hyperledger Fabric/Corda/Quorom: Three Different Distributed Leger Technologies for Business", In *International Conference on Mobile Radio Communications & 5G Networks*, pp. 383-395, Singapore: Springer Nature Singapore, (2023).

[3] G. Kumar, "Blockchain in enterprise application for pharmaceutical drug traceability," *International Journal of Science and Research*, vol. *12, no.* 8, pp. 130-134, (2023).

[4] S. B. Toumia, C. Berger and H. P. Reiser, "Evaluating blockchain application requirements and their satisfaction in Hyperledger Fabric," arXiv preprint arXiv:2111.15399, (2021).

[5] D. Ravi, S. Ramachandran, R. Vignesh, V. R. Falmari and M. Brindha, "Privacy-preserving transparent supply chain management through Hyperledger Fabric," *Blockchain: Research and Applications*, vol. 3, no. 2, pp. 100072, (2022).

[6] X. Liang, Q. Zhao, Y. Zhang, H. Liu and Q. Zhang, "EduChain: A highly available education consortium blockchain platform based on Hyperledger Fabric," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 18, pp. e6330, (2023).

[7] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. *8*, pp. 70604-70615, 2020.

[8] W. Rafique, M. Khan, S. Khan and J. S. Ally, "SECUREMED: A blockchain-based privacy-preserving framework for internet of medical things," *Wireless Communications and Mobile Computing*, vol. 2023, no. 1, pp. 2558469, (2023).

[9] K. Miyachi and T. K. Mackey, "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Information processing & management*, vol. 58, no. 3, pp. 102535, (2021).

[10] T. H. Kim, G. Kumar, R. Saha, M. K. Rai, W. Buchanan, R. Thomas and M. Alazab, "A privacy-preserving distributed ledger framework for global human resource record management: The blockchain aspect," *IEEE Access*, vol. 8, no. 96455-96467, (2020).

[11] M. A. Ghanimi, Hayder, P. Melgarejo-Bolivar Romel, A. Tumi-Figueroa, S. Ray, D. Pankaj and S. Sudhakar, "Merkle-Damgå RD hash functions and blockchains: Securing electronic health records," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 237–248, (2024).

[12] M. A., Ghanimi, Hayder. T. Gopalakrishnan, G. D. Joel Sunny, K. Amarendra, D. Pankaj and S. Sudhakar, "Chebyshev polynomial approximation in CNN for zero-knowledge encrypted data analy-

sis," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 203–214, (2024).

[13] P. Vidya Sagar, M. A. Ghanimi, Hayder, L. Prabhu Arokia Jesu Raja, D. Pankaj and S. Sudhakar, "Secure multi-party computation in deep learning: Enhancing privacy in distributed neural networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 249–259, (2024).

[14] G. R. K. Rao, M. A. Ghanimi, Hayder, V. Ramachandran, D. Al-Qahtani, D. Pankaj and S. Sudhakar, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 361–370, (2024).

[15] K. Raguru Jaya, T. Gopalakrishnan, M. Divyapushpalakshmi, K. Amarendra, D. Pankaj and S. Sudhakar, "Security and privacy concerns in social networks mathematically modified metaheuristic-based approach," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 371–382, (2024).

Received November, 2024