

# Implementing zero-knowledge proof authentication on Hyperledger fabric to enhance patient privacy and access control

Praveena Bolly Joshi, Arivazhagan Natesan

Department of Computational Intelligence, SRM Institute of Science and Technology, Kattankulathur, India

## Article Info

### Article history:

Received May 15, 2024

Revised Sep 6, 2024

Accepted Sep 29, 2024

### Keywords:

Blockchain

Hyperledger Fabric

Identity management

Privacy

Zero knowledge proof

## ABSTRACT

In recent years, the healthcare sector has encountered significant challenges in authenticating identities for online medical services. A predominant reliance on centralized identity management systems (IDMs) has presented obstacles to the seamless exchange of patient identities among various healthcare institutions, often resulting in data isolation within individual silos. Of paramount concern are the potential privacy breaches associated with centralized IDMs, which may compromise patient confidentiality. In response to these challenges, we propose a novel approach to securely sharing patient details across multiple hospitals utilizing the zero-knowledge access protocol (MediCrypt-ZKAP) within the Hyperledger Fabric blockchain framework. By adopting MediCrypt-ZKAP, hospitals can effectively verify the identities of requesting entities without disclosing sensitive patient information, thereby ensuring the highest levels of confidentiality and privacy protection. The proposed system represents a proactive step towards addressing the critical need for secure and interoperable patient data exchange within the healthcare sector. Through the integration of MediCrypt-ZKAP into existing blockchain infrastructure, our solution aims to enhance data security and privacy while promoting seamless collaboration among healthcare institutions.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Praveena Bolly Joshi

Department of Computational Intelligence, SRM Institute of Science and Technology

Kattankulathur, Tamilnadu, India

Email: pb2102@srmist.edu.in

## 1. INTRODUCTION

Sharing hospital data with stakeholders is crucial for collaboration, improving healthcare outcomes, and driving innovation. It enables researchers to conduct comprehensive studies, policymakers to make informed decisions, and healthcare providers to deliver more personalized care [1]. However, sharing such sensitive data poses significant challenges, including ensuring patient privacy and data security, which require robust encryption and compliance with stringent regulations [2]. Interoperability issues between different healthcare systems, varying data formats, and concerns regarding data accuracy and integrity add complexity. Despite these hurdles, effective data sharing is critical for advancing medical research, improving patient care, and saving lives [3].

Hyperledger Fabric safeguards patient data with its permissioned blockchain architecture, ensuring only authorized participants access sensitive information [4]. Its modular design allows customization of data access controls, maintaining confidentiality and compliance with privacy regulations [5]. Hyperledger Fabric's endorsement procedures ensure data integrity and reduce the risk of fraudulent activity.

Zero-knowledge proof (ZKP) offers a groundbreaking solution for verifying information without disclosing sensitive details, proving knowledge without revealing the underlying information. ZKP enables hospitals to verify staff identities without disclosing unnecessary personal details, minimizing the risk of data breaches or unauthorized access [6].

In the existing system, patient data is maintained on a centralized server where several threats and vulnerabilities exist, compromising the security and privacy of patient data [7]. One major threat is the risk of unauthorized access, either by internal staff members with malicious intent or external hackers exploiting system vulnerabilities [8]. Another vulnerability lies in the lack of encryption and data protection measures, leaving patient information susceptible to interception or eavesdropping during transmission over networks [9]. Furthermore, because these systems rely on centralized storage, they become a single point of failure in the event of a breach or system outage, endangering healthcare operations and access to vital patient data. Casino *et al.* [10] explored the potential of blockchain technology to improve various applications in the healthcare sector, including electronic health record (EHR) management, combating drug counterfeiting, and fostering user-centric medical research. The zk-SNARKs [11] algorithm allows one party to prove they know a value satisfying a computational statement without revealing it, using succinct, non-interactive proofs that are quickly verified. This is achieved by encoding the computation as a polynomial and generating a proof of correct evaluation, ensuring soundness and zero-knowledge. But the algorithm has the complexity and computational overhead involved in generating and verifying zk-SNARK proofs, which requires significant resources and setup time. Mell *et al.* [12] is federated identity management (IDM), which enables users from one domain can log in and use services from another. Examples include single-sign-on systems like Facebook connect. Still, these two IDM strategies typically rely on centralized servers, limiting user control. Consequently, there are significant security concerns regarding user identity, potentially resulting in data disclosure in the event of server compromise. While MeDShare [13] shares many conceptual similarities with our work, the specific blockchain framework used is not specified. Additionally, the authors primarily delve into the foundational aspects of blockchain technology, such as data blocks and smart contracts, rather than presenting a concrete solution. Genestier *et al.* [14] introduced a model wherein patients autonomously govern access consent to their data via blockchain in a decentralized manner. Despite a smart contract facilitating access control, the patient's application interacts with the blockchain through at least two centralized intermediaries.

The challenges need to be addressed: (i) Traditional identity verification methods frequently require the sharing of sensitive information [15], which can lead to potential privacy violations, data misuse, and patient data exposure throughout the verification process. (ii) Conventional authentication methods can be susceptible to replay attacks, in which a hacker intercepts and uses legitimate authentication information again [16]. (iii) Customary techniques for validating identity can require a lot of time and resource-intensive, especially in a decentralized system with multiple entities [17].

In this paper, we present a blockchain-based, fully decentralized identity authentication system for healthcare sectors based on zero-knowledge proof. The rest of this paper is structured as follows: section 2 describes the overview and the methodology of MediCrypt-ZKAP. In section 3 examines the system's performance and security. Finally, in section 4, we conclude with a summary of MediCrypt-ZKAP and discuss potential future work.

## 2. METHOD

### 2.1. Proposed authenticating system

To overcome the aforementioned difficulties our contribution is:

- a) We implement a health care zero-knowledge authenticating solution named MediCrypt-ZKAP, comprising three entities: system user, healthcare providers (Doc A), blockchain (admin), and stakeholder (Doc B). The system user, composed of patients and healthcare providers, accesses the proposed system. Users will create identity-proof information and store it on the blockchain. Healthcare providers verify user identities by querying the blockchain for relevant information. The admin initializes the blockchain, deploys the chaincode, and facilitates the trusted setup for zero-knowledge proof.
- b) We integrate Fiat-Shamir zero-knowledge proof algorithm [18], into the MediCrypt-ZKAP system to generate the user-provided identity-proof data and verify the proof data that is kept on the blockchain. Actual user information remains off the blockchain, ensuring the privacy and security of the user's data.
- c) MediCrypt-ZKAP has been implemented on the Hyperledger Fabric [19] consortium blockchain, with the chaincode deployed on Fabric for uploading and validating user identity information. Healthcare providers initiate the invocation of the chaincode whenever they verify a user's identity.
- d) We evaluate the performance of the MediCrypt-ZKAP system using Caliper [20]. The results indicate that our system can achieve a throughput exceeding 410 TPS.

- e) In the framework, we use IoT devices like temperature, heart rate, blood pressure, and SPO2 to absorb the live health status of the patient [21]. These sensors transmit data, which is then processed and securely stored within Hyperledger Fabric. In Hyperledger Fabric, we created one organization with three entities system users, healthcare providers, and admin being part of it. The health provider (Doc A) will act as the endorser who authenticates the sensor data based on threshold values using a consensus algorithm and adds it to the blockchain as a block.

We use threshold value to filter the data because IoT has lot of data and adding all the data to the blockchain is an expensive task. So, we set a threshold value and data above it will be sent to blockchain and rest to the customized repository. This works we already submitted in our previous paper. Now, we want to share this patient's health data with other hospital doctors like Doc B. So, before we share, Doc B authentication has to be done by considering all the security concerns without revealing any personal information of the doctor. To address this, we employ ZKP, a fundamental tool in cybersecurity and privacy protection. ZKP offers an innovative approach to verifying information without compromising the confidentiality of any personal details.

The proposed model for chaincode implementation in Hyperledger Fabric aims to improve the security and privacy of patient data by authenticating doctors using the MediCrypt-ZKAP (zero-knowledge access protocol) zero-knowledge proof protocol.

## 2.2. Entities

Three entities: system user, healthcare providers (Doc A), blockchain (admin), and stakeholder (Doc B). Below is a brief description of each entity:

- System users: a patient or a healthcare professional may use the suggested system. The user can upload the created identity proof data to the system and carry out the trusted setup of MediCrypt-ZKAP through the client as the owner of the identity information. Every user has a unique token that serves as a representation of their digital identity.
- Healthcare providers: healthcare providers hold responsibility for validating patient identities. The patient is verified by using their unique token generated by the Blockchain. Healthcare providers assign a set of sensors to the patient and record the data in the blockchain. They also use the proposed zero knowledge access protocol to share the patient data with the other hospital stakeholders. In our work, we use Doc A as a healthcare provider and the other hospital stakeholder will be Doc B.
- Blockchain/admin: the admin oversees system design, maintenance, and user collaboration for configuring MediCrypt-ZKAP. They ensure proper management and supervision of all participants, including public agencies and regulatory bodies. The admin also manages chaincode execution on the blockchain, verifying health status updates with healthcare providers.

## 2.3. The MediCrypt-ZKAP workflow is as follows

When invoked as per Figure 1, the function MediCrypt-ZKAP accepts the authentication token of Doctor B (Doc B) as an input parameter. The chaincode then proceeds to generate a prime number, denoted as 'p', and selects a random generator 'G'. Subsequently, it computes various cryptographic parameters, including 'u' and 'v', which are exchanged between the server, Doctor A (Doc A), and Doctor B. In this exchange, Doctor A transmits a random value 'c' to Doctor B, who then computes 'w' using the received authentication token. Following this exchange, Doctor A computes 'v\_docb' and compares it with 'v' to verify the authenticity of Doctor B. If the calculated values match, the authentication process is deemed successful, confirming Doctor B's identity. This chaincode implementation [22] ensures a robust and secure authentication mechanism for doctors within the Hyperledger Fabric network, leveraging the MediCrypt-ZKAP protocol to uphold confidentiality and integrity in healthcare data management. A detailed Algorithm 1.

### Algorithm 1. MediCrypt-ZKAP

```

1: procedure MediCrypt-ZKAP(docb_sent_AuthToken)
2:    $p \leftarrow 701$  ▷ Choose a prime number
3:    $G \leftarrow \text{random}(1, p)$  ▷ Choose a random generator
4:    $original\_AuthToken \leftarrow \text{SHA256}(docb\_sent\_AuthToken)$ 
5:    $original\_s \leftarrow \text{int}(original\_AuthToken, 16) \bmod p$ 
6:    $u \leftarrow G^{original\_s} \bmod p$  ▷ Compute u
7:   print server → doca:  $u = u$ 
8:    $t \leftarrow \text{random}(1, p)$ 
9:    $v \leftarrow G^t \bmod p$  ▷ Compute v
10:  print docb → doca:  $v = v$ 
11:   $c \leftarrow \text{random}(1, p)$ 
12:  print doca → docb:  $c = c$ 

```

```

13:   sent_AuthToken ← encode(docb_sent AuthToken)
14:   sent_s ← int(SHA256(sent_AuthToken), 16) mod p
15:   w ← (t - c × sent_s)
16:   print docb → doca: w = w
17:   if w < 0 then
18:       tm ← G-w mod p
19:       m ← tm-1 mod p
20:   else
21:       m ← Gw mod p
22:   end if
23:   n ← uc mod p
24:   v_docb ← (m × n) mod p
25:   print doca computed v = v_docb
26:   if v = v_docb then
27:       print Success: docb is authenticated !!!
28:   else
29:       print Failure: docb is not authenticated !!!
30:   end if
31: end procedure
    
```

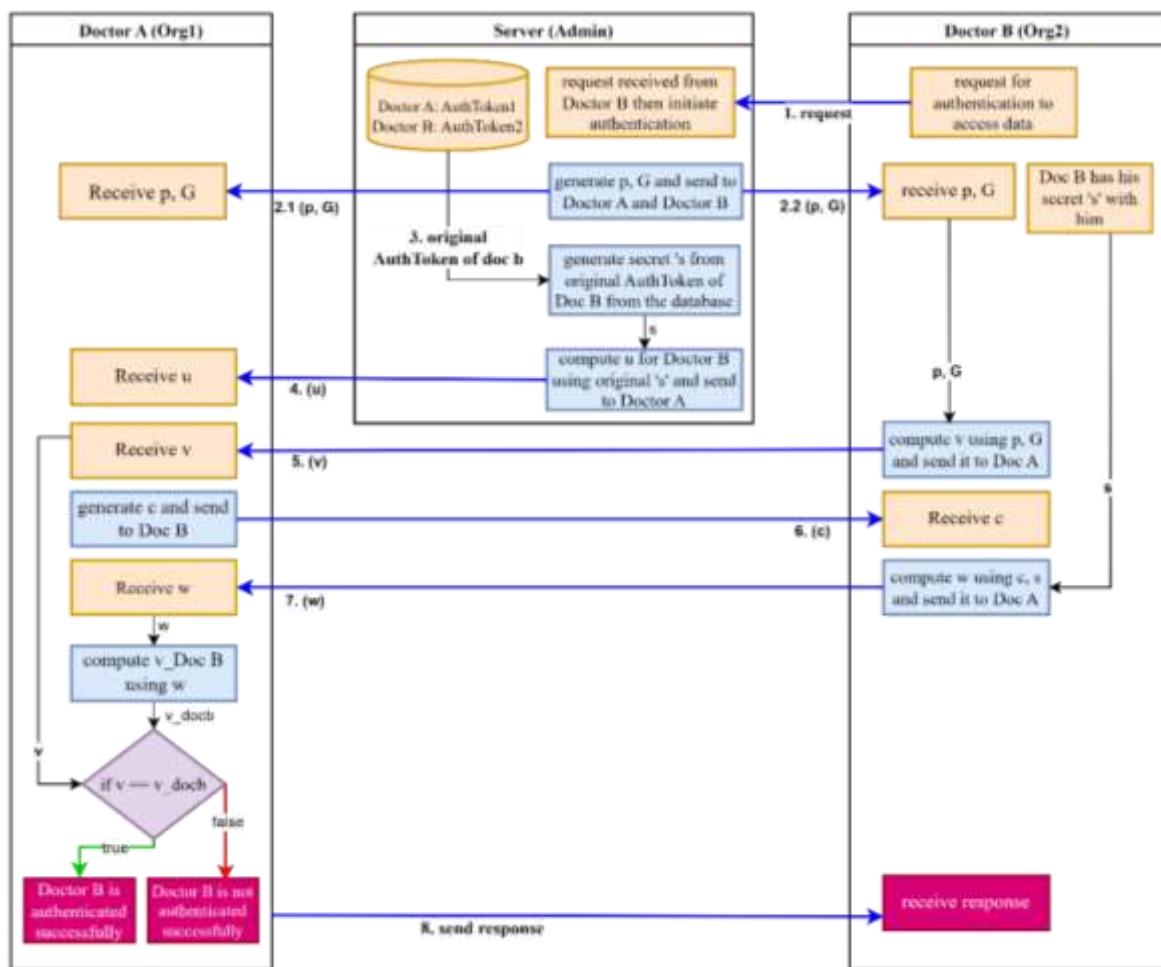


Figure 1. The proposed model of MediCrypt-ZKAP

### 3. RESULTS AND DISCUSSION

A zero-knowledge proof system must ensure that if the witness statement is valid, the prover can always satisfy the verifier (completeness), and a benevolent prover is unable to convince the verifier that a statement is false (soundness). Additionally, the verifier should only learn that the statement is true without gaining any specific knowledge about the statement itself (zero-knowledge).

- The challenge  $c$  is randomly generated by the verifier (line 11). This randomness ensures that a dishonest prover cannot predict or influence the challenge.

- The value  $u \leftarrow G^{\text{original}_s} \bmod p$  (line 6) binds the prover to a specific value based on their secret  $\text{original}_s$ .
- The verification step checks if  $v = v_{docb}$  where  $v_{docb} \leftarrow (m \times n) \bmod p$  computed using the prover's response and the original commitment (line 24). If the prover does not know the secret  $\text{sent}_s$ , they cannot produce a valid result that will satisfy this equation and ensures the completeness.

The protocol's soundness and completeness [23] is ensured by the use of random challenges, binding commitments, and the proper verification of the prover's response. This prevents a dishonest prover from successfully authenticating without knowing the correct authorization token.

The proposed work is deployed on processor 11th Gen Intel(R) Core (TM) i5-11400H @ 2.70GHz 2.69 GHz and Ubuntu Linux 20.04/22.04 LTS (both 64-bit) operating systems with 4 GB RAM and 40 GB disk space [24]. A permissioned Hyperledger Fabric (HLFv2.0) network was set up with one Channel connecting two organizations Org1, and Org2. Doc A is part of Org1 and Doc B is part of Org2 as peers. The chaincode prototype in the system is written in Golang. The client framework is MediCrypt-ZKAP + Golang + Html.

Doc A, as the healthcare provider, holds access to patient health records, for example, those of patient 1. When Doc A seeks a second opinion or evaluation from another doctor (Doc B), they initiate the process of sharing the patient's records. Doc B as in Figure 2, has to register to the framework which generates a unique token. Eg: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MTUzODY1MjAsInVzZXJuYXV1IjoiZG9jYjEiLCJvcmdOYW11IjoiaT3JnMSIsImhhbmciOiJMTc3NTM1MDUyMH0.bOOhy9CW5xEYmLtiJZSxYXz0kevznEEk8aPAUxq3jqs".

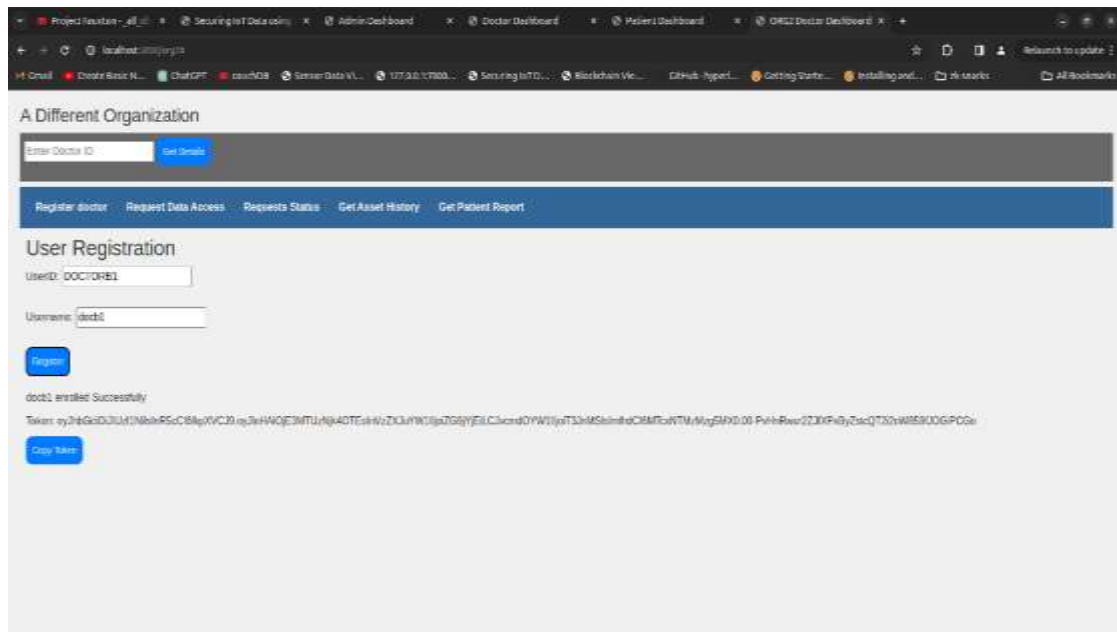


Figure 2. Doc B registration information

When Doc B's registration information is transmitted to Doc A for authentication, Doc A utilizes the MediCrypt-ZKAP (zero knowledge access protocol) to validate the legitimacy of the request, utilizing Doc B's unique token, as illustrated in Figure 3. Upon receiving the request, Doc A has two possible actions: discard or start authentication. When opting to begin the authentication process, the MediCrypt-ZKAP chaincode is activated. It processes the Doc B token while factoring in the prime number and random numbers according to the algorithm. If the authentication fails the health provider can use a discard action to deny access to the health records. CouchDB [25] is used to maintain the blockchain data which is well integrated to HLFv2.0.

After the zero-knowledge access protocol successfully authenticates the doctors, the patient details are then shared with them as in Figure 4. Figure 5 illustrates the access granted to Doc B following the validation by the zero-knowledge access protocol.



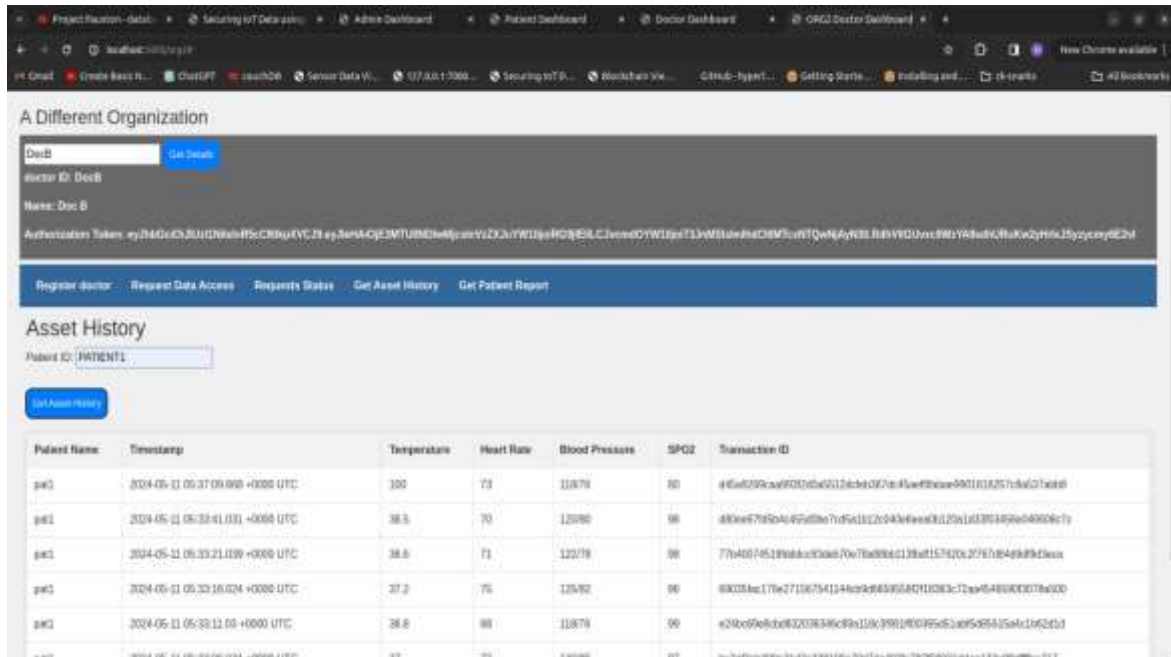


Figure 5. Depicts the authorization granted to Doc B

### 3.1. Performance analysis

In this test scenario the test was conducted for creating numerous user accounts in the network. Hyperledger Caliper [20] is used to evaluate the performance. For creating user accounts, we used 400 user accounts with 200 transactions per second (TPS). Table 1 shows the test results. We investigated the effect of the number of peers on blockchain efficiency, where peers indicate the number of users processing transactions simultaneously. Table 1 illustrates the association among the number of peers and TPS. The TPS gradually lowers as the number of peers increases. To obtain high TPS, fewer peers are necessary. However, in reality, there are a large number of peers representing both patients and medical professionals. “In comparison to the literature [20], the throughput is increased by two to threefold.

Table 1. Caliper report of Fabric performance

| Name                  | Succ | Fail | Send rate (TPS) | Max latency (s) | Min latency (s) | Avg latency (s) | Throughput (TPS) |
|-----------------------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|
| Create account        | 2500 | 0    | 200             | 4.28            | 0.32            | 2.35            | 410.1            |
| Insert transactions   | 2497 | 3    | 200             | 6.32            | 1.23            | 3.77            | 381.2            |
| Querying transactions | 2500 | 0    | 200             | 1.12            | 0.68            | 0.96            | 396.2            |

The algorithm effectively addresses key issues inherent in traditional identity verification methods. Firstly, by utilizing cryptographic hashes and modular arithmetic, MediCrypt-ZKAP ensures that sensitive information, such as the authentication token, is never directly shared. Instead, only derived cryptographic values are exchanged, significantly reducing the risk of privacy violations, data misuse, and patient data exposure. Secondly, the algorithm mitigates the risk of replay attacks through the use of random challenges and nonces in each verification session. This ensures that even if an attacker intercepts valid authentication data, they cannot reuse it to gain unauthorized access, as the challenge-response mechanism guarantees the freshness of each authentication attempt.

Thirdly, MediCrypt-ZKAP streamlines the identity validation process, making it less time-consuming and resource-intensive. Traditional methods often involve extensive data exchanges and complex procedures, particularly in decentralized systems with multiple entities. In contrast, MediCrypt-ZKAP’s efficient and deterministic computations ensure quick verification without compromising security. This makes the algorithm particularly advantageous in decentralized healthcare systems where rapid and reliable identity verification is critical. By addressing these fundamental issues, MediCrypt-ZKAP provides a robust, efficient, and privacy-preserving alternative to conventional authentication methods.

#### 4. CONCLUSION

The MediCrypt-ZKAP algorithm addresses several limitations of traditional zero-knowledge proof (ZKP) systems through its streamlined and efficient approach. By employing basic cryptographic operations and modular arithmetic, it reduces computational overhead and ensures faster execution times compared to more complex ZKP protocols like zk-SNARKs. This simplicity makes MediCrypt-ZKAP well-suited for resource-constrained environments while maintaining robust security. Furthermore, the algorithm's compact message exchange optimizes communication efficiency, reducing the bandwidth required for interactions between the prover and verifier. These features collectively enhance the practicality and scalability of MediCrypt-ZKAP in various authentication scenarios.

Looking towards future enhancements, several avenues could further improve MediCrypt-ZKAP's capabilities. Increasing the size of the prime number  $p$  could enhance security by making the cryptographic operations more resistant to attacks. Additionally, integrating advanced random number generators would strengthen the robustness of the algorithm against potential vulnerabilities. Another potential enhancement could involve combining MediCrypt-ZKAP with other cryptographic protocols to create a comprehensive security framework, addressing a broader range of security challenges. Continuous adaptation and innovation will ensure that MediCrypt-ZKAP remains a cutting-edge solution in the evolving landscape of ZKP and cryptographic authentication.

#### REFERENCES





- [1] T. Bai, Y. Hu, J. He, H. Fan, and Z. An, "Health-zkIDM: a healthcare identity system based on fabric blockchain and zero-knowledge proof," *Sensors (Basel, Switzerland)*, vol. 22, no. 20, p. 7716, Oct. 2022, doi: 10.3390/s22207716.
- [2] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security and Privacy*, vol. 16, no. 4, pp. 20–29, Jul. 2018, doi: 10.1109/MSP.2018.3111247.
- [3] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022, doi: 10.1007/s00521-020-05519-w.
- [4] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.
- [5] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," *Proceedings - 26th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, MASCOTS 2018*, pp. 264–276, 2018, doi: 10.1109/MASCOTS.2018.00034.
- [6] Z. Mahmood and J. Vacius, "Privacy-preserving block-chain framework based on ring signatures (RSs) and zero-knowledge proofs (ZKPs)," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT 2020*, Dec. 2020, pp. 1–6, doi: 10.1109/3ICT51146.2020.9312014.
- [7] Q. Wang and S. Qin, "A hyperledger fabric-based system framework for healthcare data management," *Applied Sciences (Switzerland)*, vol. 11, no. 24, p. 11693, Dec. 2021, doi: 10.3390/app112411693.
- [8] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. ur-Rehman, and C. A. Kerrache, "The case of HyperLedger Fabric as a blockchain solution for healthcare applications," *Blockchain: Research and Applications*, vol. 2, no. 1, p. 100012, Mar. 2021, doi: 10.1016/j.bcr.2021.100012.
- [9] R. Anusuya, D. K. Renuka, S. Ghanasiyaa, K. Harshini, K. Mounika, and K. S. Naveena, "Privacy-preserving blockchain-based EHR using ZK-Snarks," in *Communications in Computer and Information Science*, vol. 1631, 2022, pp. 109–123.
- [10] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.
- [11] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, " Succinct non-interactive zero knowledge for a von neumann architecture," *Proceedings of the 23rd USENIX Security Symposium*, pp. 781–796, 2014.
- [12] P. Mell, J. Dray, and J. Shook, "Smart contract federated identity management without third party authentication services," *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI)*, vol. P-293, pp. 37–48, 2019.
- [13] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017, doi: 10.1109/ACCESS.2017.2730843.
- [14] P. Genestier *et al.*, "Blockchain for consent management in the ehealth environment: a nugget for privacy and security challenges," *Journal of the International Society for Telemedicine and Ehealth*, 2017, [Online]. Available: <https://journals.ukzn.ac.za/index.php/JISfTeH/article/view/269%0Ahttps://journals.ukzn.ac.za/index.php/JISfTeH/article/download/269/754>.
- [15] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: a BLOCKchain-based platform for healthcare information exchange," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, Jun. 2018, pp. 49–56, doi: 10.1109/SMARTCOMP.2018.00073.
- [16] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BioTHR: electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857–10872, Jul. 2021, doi: 10.1109/IIOT.2021.3050703.
- [17] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, Aug. 2019, doi: 10.1109/TCE.2019.2926192.
- [18] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.
- [19] A. R. Rajput, Q. Li, and M. T. Ahvanooy, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," *Healthcare (Switzerland)*, vol. 9, no. 2, p. 206, Feb. 2021, doi: 10.3390/healthcare9020206.
- [20] "Hyperledger Caliper." <https://github.com/hyperledger/caliper>.
- [21] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-id: a blockchain-based decentralized identity management for remote healthcare," *Healthcare (Switzerland)*, vol. 9, no. 6, p. 712, Jun. 2021, doi: 10.3390/healthcare9060712.







- [22] D. A. Jones, J. P. Shipman, D. A. Plaut, and C. R. Selden, "Characteristics of personal health records: findings of the medical library association/national library of medicine joint electronic personal health record task force," *Journal of the Medical Library Association*, vol. 98, no. 3, pp. 243–249, 2010, doi: 10.3163/1536-5050.98.3.013.
- [23] A. Roehrs, C. A. Da Costa, R. D.-R. Righi, and K. S. F. De Oliveira, "Personal health records: a systematic literature review," *Journal of Medical Internet Research*, vol. 19, no. 1, p. e13, Jan. 2017, doi: 10.2196/jmir.5876.
- [24] M. B and H. C., "Polynomial commitment-based zero-knowledge proof schemes," *AIJR Preprints*, 2022, doi: 10.21467/preprints.384.
- [25] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: a review," *Journal of Network and Computer Applications*, vol. 166, p. 102731, Sep. 2020, doi: 10.1016/j.jnca.2020.102731.

## BIOGRAPHIES OF AUTHORS



**Praveena Bolly Joshi**     is a research scholar at SRMIST Chennai, she holds an M.Tech. in Computer Science and Engineering from JNTU and has 20 years of teaching experience. With approximately 15 papers published in international journals and conferences, her research interests lie in network security and blockchain technology. Additionally, she is a member of IEEE and ISTE. She can be contacted at email: pb2102@srmist.edu.in.



**Dr Arivazhagan Natesan**     is associate professor in the Department of Computational Intelligence, Faculty of Engineering and Technology, Kattankulathur–Chennai, Tamil Nadu. Ph.D., in Machine Learning - Computer Science in 2020 from SRM Institute of Science and Technology, Kattankulathur Tamilnadu. He has done his M.S, in Systems and Information from Birla Institute of Technology, Pilani, in the year 1995. Dr N Arivazhagan has 34 years of teaching experience and has 20 publications in International Journals and Conferences. His research interests include machine learning and medical image processing. He is an active member of ACM, I ISTE, and IEANG. He can be contacted at email: arivazhn@srmist.edu.in.