Journal of Hunan University

(Natural Sciences)

Vol. 52 No. 12

December 2025

Available online at

https://jonuns.com

Open Access Article

https://doi.org/10.55463/issn.1674-2974.52.12.10

A Smart Contract-Based Multi-Factor Authentication Mechanism for Secure Tracking of Medical Records

Zouhair Elhadari[1*], Hicham Zougagh[1], Noureddine Idboufker[2], Mohamed Ech-chebaby[1], Samir elouaham[3]

[1] Computer Science Department, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco,

[2] Telecommunications and Computer Sciences Department, National School of Applied Sciences, Cady Ayyad University, Marrakech, Morocco,

[3] Physics Department, Faculty of Sciences, Chouaib Doukkali University, Eljadida, Morocco,

* Corresponding author: zouhair.hdr@gmail.com

Article history
Received: November 7, 2025
Revised: December 14, 2025
Accepted: January 6, 2026
Published: January 30, 2026

Abstract: The digitization of medical records in the healthcare sector demands robust mechanisms to ensure data confidentiality, integrity, and privacy. This paper proposes an innovative multi-factor authentication (MFA) mechanism that leverages smart contracts and blockchain technology to secure the tracking of medical records. The proposed system, named Blockchain Authentication with Zero-Knowledge Proof (BAZKP), provides a tamper-proof environment for storing and accessing records while preserving users' personally identifiable information (PII). A key novelty of BAZKP lies in storing only the character count structure of passwords rather than the actual credentials, combined with zero-knowledge proofs (ZKP) to verify identity without exposing sensitive data. This hybrid blockchain/ZKP approach addresses limitations of centralized and hardware-based solutions, reducing vulnerabilities while avoiding the cost and usability constraints of dedicated hardware systems.
The system was implemented and tested on a private Ethereum testnet, with a proof-of-concept application developed using Solidity, Web3.js, and MetaMask. Performance evaluation over 100 transactions for core operations (registration, login, and password reset) demonstrated practical viability: registration incurred the highest latency (≈4500 ms) and gas consumption (≈120,000 gas), while login and reset operations were more efficient (≈4000 ms/80,000 gas and ≈3500 ms/60,000 gas, respectively). Comparative security analysis against existing MFA

methods—including 2FA, hardware tokens, and biometrics—confirms that BAZKP provides superior privacy protection through decentralization and ZKP, without the cost and usability drawbacks of hardware-based solutions. Overall, this approach enhances trust in digital health systems by offering a secure, transparent, and privacy-preserving authentication framework for medical data, representing a significant advancement in digital healthcare security.

Keywords: Blockchain; Multi-Factor Authentication; Smart Contracts; Zero-Knowledge Proof; Medical Record Security.

基于智能合约的多因素认证机制用于医疗记录的安全追踪

摘要：医疗行业的病历数字化要求具备强大的机制，以确保数据的机密性、完整性和隐私性。本文提出了一种创新的多因素认证（MFA）机制，结合智能合约与区块链技术，用于保障病历的安全追踪。该系统命名为“基于区块链与零知识证明的认证”（Blockchain Authentication with Zero-Knowledge Proof，BAZKP），能够在保障用户个人身份信息（PII）的前提下，提供篡改防护的记录存储与访问环境。

BAZKP 的核心创新在于仅存储密码的字符计数结构，而非实际凭证，并结合零知识证明（ZKP）进行身份验证，从而无需暴露敏感数据。这种区块链/ZKP 混合方法解决了集中式及硬件依赖方案的局限性，在降低系统漏洞的同时避免了硬件成本和使用约束。

系统已在私有以太坊测试网络上实现，并通过 Solidity、Web3.js 与 MetaMask 开发了概念验证应用。对核心操作（注册、登录及密码重置）的 100 次交易性能评估显示系统具有实际可行性：注册操作延迟最高（约 4500 毫秒）且燃气消耗最高（约 120,000 gas），而登录与重置操作效率较高（约 4000 毫秒/80,000 gas 和 约 3500 毫秒/60,000 gas）。

与现有 MFA 方法（包括二次验证、硬件令牌和生物识别）比较分析表明，BAZKP 通过去中心化与零知识证明提供更优的隐私保护，同时避免了硬件方案的成本和可用性缺陷。总体而言，该方法为数字医疗系统提供了安全、透明且隐私保护的认证框架，显著提升了数字健康数据的信任度，代表了数字医疗安全领域的重要进展。

关键词：区块链；多因素认证；智能合约；零知识证明；病历安全

1. Introduction

The healthcare sector's growing reliance on electronic medical records (EMRs) has significantly improved patient care and operational efficiency [1]. However, this digital transformation has simultaneously intensified security and privacy concerns for sensitive patient data. The increasing interconnectivity of healthcare systems has elevated risks of unauthorized access and data breaches [2], demanding stronger protective measures [3].

Multi-factor authentication (MFA) has emerged as a critical component in safeguarding access to medical records, providing an additional layer of security beyond traditional password-based systems. By requiring multiple forms of verification, MFA significantly reduces the likelihood of unauthorized access [4], thereby protecting patients' personal identifiable information (PII) from cyber threats.

This paper presents a blockchain-based MFA solution for medical record tracking, utilizing smart contracts to establish a tamper-proof access

management framework. The system incorporates zero-knowledge proofs to enable secure identity verification while maintaining complete data confidentiality.

The major contributions of this work are as follows:

- Overview of Current Challenges: Discuss the existing challenges in securing medical records, including unauthorized access, data breaches, and the inadequacy of traditional authentication methods.
- Proposed MFA Mechanism: Introduce the smart contract-based MFA mechanism, which stores character counts of passwords instead of actual passwords, ensuring that sensitive information is not compromised.
- Integration with Healthcare Systems: Explore how this mechanism can be integrated into existing healthcare systems to facilitate secure access to medical records by authorized personnel while maintaining patient privacy.
- Use of Zero-Knowledge Proofs: Explain how zero-knowledge proofs can be utilized to verify user credentials without revealing any sensitive information, thus enhancing security.
- Case Studies and Applications: Provide examples of how this mechanism can be applied in real-world healthcare scenarios, such as telemedicine, patient data sharing, and emergency access to medical records.
- Theoretical implications: This work contributes to the literature by demonstrating the practical applicability of ZKPs in large-scale medical authentication scenarios, paving the way for zero-trust architectures in digital health ecosystems.

This research selected the blockchain/ZKP approach based on three main criteria:

- The ability to provide identity verification without exposing sensitive data.
- The elimination of single points of failure typical of centralized systems.
- Alignment with strict medical data protection regulations (HIPAA, GDPR).

The paper is organized into seven sections. Section 2 discusses the related works in multi-factor authentication used in smart healthcare. In Section 3 we provide an overview of the major security issues in a smart healthcare ecosystem and discusses the need for MFA in this ecosystem. Section 4 provides a description of the proposed MFA approach based on the concept of smart contracts. Section 5 presents an exploration of the key findings. Section 6 provides a discussions and futures directions of the proposed MFA. Finally, we conclude the work with the main conclusions in Section 7.

2.Related Works

MFA has advanced considerably to address rising security demands across sectors like healthcare. While traditional username-password methods fail against modern cyber threats, researchers have developed stronger MFA solutions to enhance protection. Recent studies [5] highlight the effectiveness of MFA in securing EMRs, particularly through biometric authentication (e.g., fingerprints, facial recognition), which enhances security while maintaining usability. Moreover, the study [6] demonstrates that one-time passwords (OTPs) significantly reduce unauthorized access risks in healthcare settings by providing time-sensitive verification. In addition to these methods, study [7] explore blockchain's potential in authentication, leveraging decentralization and smart contracts to improve EMR security without compromising privacy. Furthermore, study [8] has shown that Combining multiple authentication factors (passwords, smart cards, biometrics) enhances security in healthcare apps. In this research [9], the implementation of such multi-layered security measures is crucial in addressing the vulnerabilities associated with single-factor authentication systems. Research [10] shows healthcare workers acknowledge MFA's security benefits but report usability challenges, calling for systems that optimize both protection and ease of use. The findings in this paper [11] emphasize that as cyber threats evolve, advanced MFA solutions will be critical in safeguarding sensitive healthcare data.

3. Overview Of Smart Healthcare Security Issues And The Need Of MFA Systems

3.1 Smart Healthcare and Underlying Security Issues

The concept of smart healthcare involves integrating advanced technologies to improve care quality, service efficiency, and patient experience [12]. This interconnected ecosystem of medical devices, health applications, and information systems enables real-time data collection and sharing, but simultaneously introduces significant security and data protection challenges [13]. Traditional password-based authentication has become inadequate for protecting sensitive patient data in increasingly digital healthcare environments. Smart healthcare systems managing large volumes of personal information are particularly vulnerable to cyberattacks, necessitating robust security solutions [14]. MFA addresses these vulnerabilities by combining multiple verification methods (passwords, SMS codes, biometrics) to create stronger protection against unauthorized access [15]. This is especially critical as healthcare professionals and patients increasingly access records through internet-connected devices [16]. Furthermore, data protection regulations, such as the GDPR in Europe [17] and HIPAA in the United States [18], impose strict requirements regarding the security of personal information. Integrating multi-factor authentication can assist

healthcare institutions in complying with these standards, ensuring that only authorized individuals can access sensitive patient information. In summary, MFA represents an essential security measure for smart healthcare systems, effectively balancing enhanced protection with the confidentiality needs of patient data in our increasingly connected medical landscape.

3.2 The Need for MFA in Secure Tracking of Medical Records

As healthcare increasingly adopts digital systems like EMRs, protecting sensitive patient data from breaches and unauthorized access has become critical. MFA is essential to strengthen medical record security in this vulnerable landscape [19]. Traditional password-based authentication is insufficient against modern cyber threats. MFA addresses this by requiring multiple verification factors knowledge (password), possession (mobile device), and inherence (biometrics) creating a robust security barrier [20]. The integration of MFA in healthcare systems not only helps to safeguard sensitive medical records but also builds trust among patients. Patients are more likely to share their information when they know that their data is protected by advanced security measures [21]. Furthermore, the adoption of MFA can assist healthcare organizations in complying with regulatory requirements related to data protection and privacy, such as HIPAA in the United States.As the healthcare landscape continues to evolve with the increasing use of telemedicine and mobile health applications, the need for secure access to medical records becomes even more critical. MFA can effectively mitigate the risks associated with remote access and ensure that only authorized personnel can view or modify patient information [22]. In conclusion, MFA is indispensable for safeguarding medical records, addressing evolving security challenges while ensuring data integrity and confidentiality in healthcare's digital transformation.

4. Proposed Approach

With the rise in cyber threats and data breaches, it is crucial to develop authentication systems that not only protect users' PII but also offer a seamless user experience. The Blockchain Authentication with Zero-Knowledge Proof (BAZKP) mechanism is proposed as an innovative solution that leverages smart contracts and zero-knowledge proof (ZKP) technology to ensure secure and privacy-preserving authentication.

4.1 System Architecture Overview

BAZKP employs a three-tier architecture that separates concerns while ensuring secure and efficient authentication, as illustrated in Figure 1:

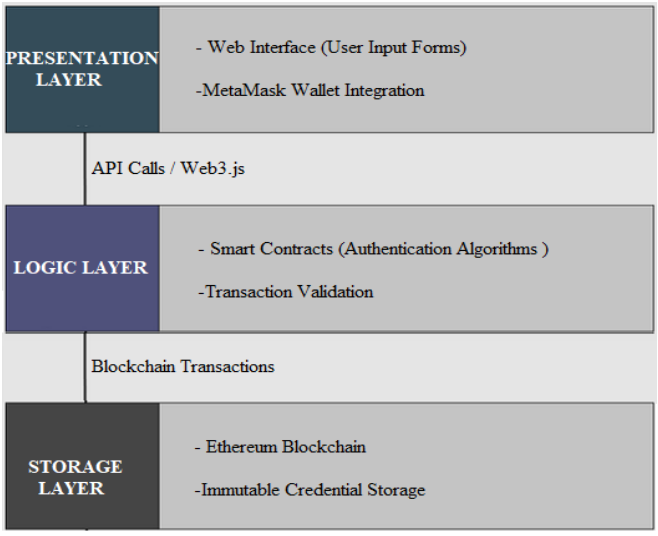

Figure 1. Three-Tier Architecture of the BAZKP System

The presentation layer provides the user interface for authentication operations. Implemented as a web application using HTML5 and JavaScript, this layer integrates with MetaMask for blockchain wallet management and includes forms for registration, login, and password reset operations. Real-time performance metrics are displayed to users, showing transaction latency, gas consumption, and costs.

The logic layer contains the core authentication intelligence implemented as Ethereum smart contracts. This layer executes Algorithms 1-4, manages the character-frequency verification engine, validates user inputs, and emits authentication events for audit purposes. Smart contracts in this layer are written in Solidity v0.8.0 and deployed to the Ethereum blockchain.

The storage layer consists of the Ethereum blockchain itself, providing immutable storage for authentication credentials and transaction records. This decentralized storage ensures that credential hashes and character-frequency proofs cannot be altered or deleted, creating a tamper-proof audit trail of all authentication events.

4.2 System Process Flow

BAZKP is based on an architecture where users' passwords are not stored in plain text. Instead, the system only records the count of each character in the password and the user's blockchain address. The process works as follows:

- User Registration: During registration, the user enters their password. The system calculates the count of each character (e.g., the number of letters, digits, symbols) and stores this information as a hash on the blockchain.
- Authentication: During login, the user provides their password. The system performs the same character count calculation and compares the resulting

hash with the one stored on the blockchain. If the hashes match, the user is authenticated.

The BAZKP system is grounded in combinatorial mathematics and information theory. For any password P composed of n characters $c1,c2,...,cn$ from alphabet A (where $|A|=256$ for ASCII), we define:

$$Freq(P)= \{(a, count_P(a)) \mid \forall a \in A\} \quad (1)$$

where $count_P(a)$ represents the frequency of character a in password P.

This method ensures that even if the database is breached, attackers cannot access the actual passwords since only the character count structure is stored. To further strengthen security, BAZKP integrates ZKP, it allows a user to prove they know a secret (in this case, their password) without revealing the secret itself. The process works as follows:

- ZKP Protocol: During authentication, the system generates a challenge that the user must solve using their password. The user responds to this challenge without ever revealing the password, thereby proving their identity. The zero-knowledge verification proof is computed as:

$$ZKP\text{-}Proof(P)=H(Freq(P)) \quad (2)$$

where H denotes the keccak256 cryptographic hash function.

This layer of privacy ensures that BAZKP is resilient against eavesdropping, replay attacks, and credential theft, and other attacks since, even if an attacker intercepts the communication, they cannot obtain the password. And the use of smart contracts play a critical role in the implementation of BAZKP, providing three critical benefits:

- Automation: Smart contracts automate the authentication process, reducing the need for human intervention and minimizing errors [23], [27].
- Transparency and Traceability: Each authentication transaction is recorded on the blockchain, offering full traceability and transparency, which builds user trust [24].
- Immutability: Once a smart contract is deployed on the blockchain, it cannot be altered, protecting the system against malicious tampering [28].

By combining these features, BAZKP ensures a trustless, tamper-proof system where users retain control over their credentials without relying on centralized authorities. BAZKP represents a paradigm shift in authentication, merging blockchain transparency, ZKP privacy, and smart contract efficiency. Unlike traditional systems, it mitigates password theft risks, resists phishing, and operates without storing sensitive data making it a next-generation solution for secure digital identity.

4.3 Algorithm Specifications

In our proposed approach, four main process are integral to the algorithm of BAZKP. This algorithm includes sign-up/registration process, login process, ZKP verification process, password reset process. The following sections provide an overview of this algorithm.

The algorithms described rely on smart contracts based on ZKP, utilizing a secure sign-up process and an enhanced login mechanism that incorporates ZKP verification. This system employs a commitment scheme to safeguard user authentication. Only users validated through the BAZKP mechanism can prove their identity to the server using a character-count-based zero-knowledge proof.

During the sign-up phase, users provide their blockchain address and a chosen password. The detailed registration process is outlined in Algorithm 1, where the password is immediately hashed to ensure security and the system calculates the character count of the password Freq(Pwd). These details, linked to the blockchain address, are stored in a blockchain-compatible database as part of the ZKP system.

Algorithm 1: Sign-Up/Registration Process

```
Input: blockchain address (BCadd), password (Pwd)
Output: Hashed password (Hpwd), character count
(Ccount) stored in the legacy database
Begin:
Hpwd ← Hash(Pwd)
Ccount ← Freq(Pwd)
Store (BCadd, Hpwd, Ccount) in DB)
Return "User registered successfully"
End
```

In the login process, when a user enters their blockchain address and password, the system hashes the entered password and compares it with the one stored during sign-up. The detailed authentication procedure is outlined in Algorithm 2. If the two hashes match, an additional step verifies the character count of the entered password against the stored value. If this verification is successful, the user is authenticated, otherwise, authentication fails.

Algorithm 2: Login Process

```
Input: blockchain address (BCadd), password (Pwd)
Output: Authentication status
Hash_entered_pwd ← Hash(Pwd)
Hah_stored ← RetrieveHash(BCadd)
Begin:
if Hah_entered_pwd == Hah_stored then
      return ZKP_Verification(Pwd)
else
      return "Authentication Failed"
end if
End
```

To enhance security, the ZKP verification process ensures that the character count of the entered password matches the stored value precisely. This step validates the user's identity without disclosing the password or any sensitive information. The detailed verification mechanism is outlined in Algorithm 3.

Algorithm 3: ZKP Verification Process

Input: Entered password (Pwd)
Output: Verification status
Begin:
Ccount' ← Freq(Pwd)
Ccount ← RetrieveCcount(BCadd)
if Ccount' == Ccount then
    return "User Verified"
else
    return "User Not Verified"
end if
End

Lastly, in cases where authentication information is lost or compromised, the password reset process allows the user to set a new password. The detailed procedure for this security update is outlined in Algorithm 4. Once entered, the new password is hashed, its character count is calculated, and the old data in the database is updated. This ensures that only the most secure and up-to-date credentials are maintained.

Algorithm 4: Password Reset Process

Input: Blockchain address (BCadd), new password (Pwdnew)
Output: Success message
Begin:
Hnew ← Hash(Pwdnew)
Ccount_new ← Freq(Pwdnew)
Update (BCadd, Hnew, Ccount_new) in DB
Return "Password reset successfully"
End

5. Implementation And Result

In the context of the increasing digitization of medical records, the need for a robust and secure authentication mechanism is more pressing than ever. This work has proposed a MFA mechanism based on smart contracts, specifically designed for the secure tracking of medical records. By integrating blockchain technology and ZKP, our approach aims to ensure the confidentiality and integrity of patients' personal information while facilitating secure access to medical data.

5.1 Implementation Environment

The implementation of the BAZKP mechanism is based on an integrated architecture that combines multiple advanced technologies to ensure secure and privacy-preserving authentication. The table 1 summarizes the main tools used at each stage of implementation.

Table 1. The main implementation tools

Stage	Tools Used
Smart Contract Development	Solidity (Creation of smart contracts to manage user authentication.)
Blockchain Interaction	Web3.js (Integration of a library to enable communication between the frontend and the blockchain.
User Authentication	MetaMask (Use of a browser extension to manage Ethereum addresses and sign transactions.)
Testing and Deployment	Truffle, Ganache (Utilization of tools for development and simulation of a local blockchain environment.)

The proposed model introduces an innovative privacy-preserving authentication method. This approach ensures a secure, efficient, and user-controlled authentication process. By integrating the Metamask wallet, a browser extension, users retain full control over their credentials, which are securely signed and validated during each interaction.

To demonstrate the functionality of this model, a proof-of-concept application was developed, as illustrated in Figure 2, showcasing its primary features.

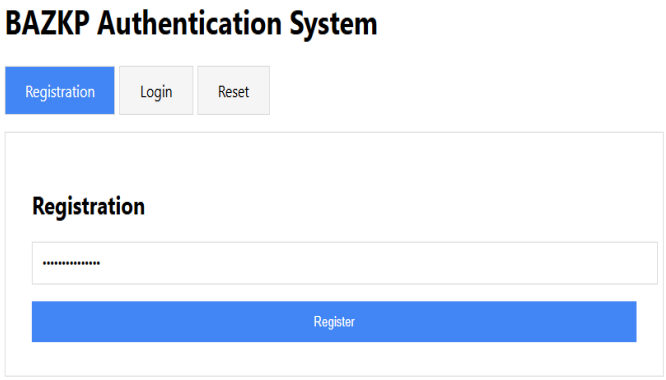

Figure 2. Web interface of the BAZKP authentication system, showing the user registration, login and reset forms

During the registration phase, users input their password and initiate the registration by clicking the "Register" button, this action triggers a Metamask popup window, requiring the user to confirm the transaction, as shown in Figure 3.

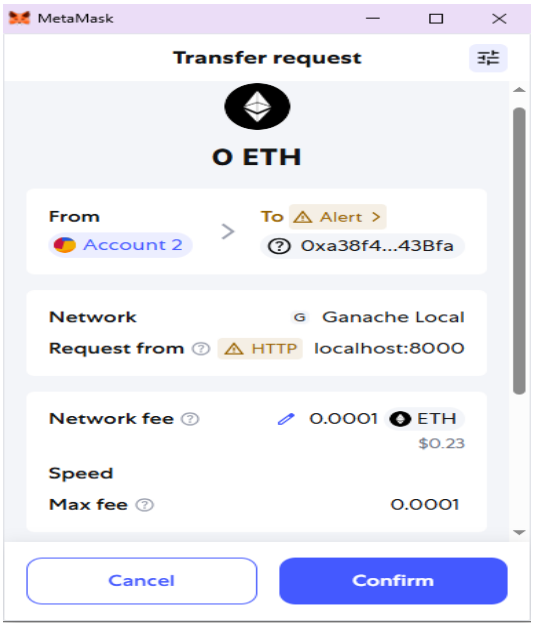

Figure 3. MetaMask wallet pop-up window prompting the user to confirm the transaction during the registration process

In our testing scenario, the deployed smart contracts on the test network are shown in Figure 4.

```
Deploying 'BAZKP_Medical'
-------------------------
> transaction hash:    0x9285f9f604b1e8e338fa1cf107ef488d34c8777b55a6de02c696eee23715cc6d
> Blocks: 0            Seconds: 0
> contract address:    0xBC826ee860aa238546709a20052Ccc36cd83b94f
> block number:        1
> block timestamp:     1754818858
> account:             0x0a48e9D0311d11a5b5d669F51c1192259bB46A12
> balance:             999.98995678
> gas used:            502161 (0x7a991)
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.01004322 ETH
```

Figure 4. List of smart contracts deployed on the private Ethereum test network

The users can add/store their password into the smart contract using Metamask, the password will be stored in the Ethetreum network against the key Ethereum Address as show in figure 5.

```
Transaction: 0x9285f9f604b1e8e338fa1cf107ef488d34c8777b55a6de02c696eee23715cc6d
Contract created: 0xbc826ee860aa238546709a20052ccc36cd83b94f
Gas usage: 502161
Block number: 1
Block time: Sun Aug 10 2025 11:40:58 GMT+0200 (heure d'été d'Europe centrale)
```

Figure 5. Example transaction record showing the hashed password data stored on the Ethereum blockchain against a user's address

5.2. Performance Metrics Analysis

To comprehensively assess the practical viability of the BAZKP mechanism, we conducted extensive performance testing involving 100 transactions for each core operation. The evaluation focused on three critical metrics: transaction latency, gas consumption, and associated costs, providing insights into the system's efficiency and economic feasibility.

The latency measurements, averaged over 100 transactions, reveal distinct temporal characteristics for each operation are shown in Figure 6. The registration process demonstrated the highest latency at approximately 4500 ms, attributable to the initial smart contract deployment and comprehensive character count calculation. Login operations exhibited moderate latency around 4000 ms, reflecting the ZKP verification overhead. Password reset operations showed the lowest latency at approximately 3500 ms, benefiting from optimized update mechanisms.

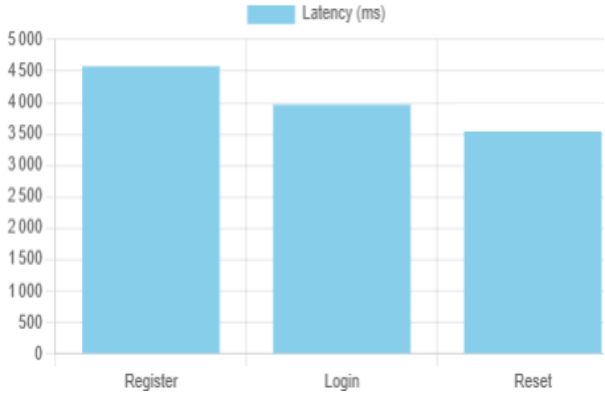

Figure 6. Average latency vs operation

Gas usage patterns are shown in Figure 7 indicate that registration consumed approximately 120,000 gas units, representing the most computationally intensive operation due to initial storage allocation and hash computation. Login operations required approximately 80,000 gas units, primarily for ZKP verification and character count comparison. Password reset operations consumed approximately 60,000 gas units, leveraging existing contract structures for updates.

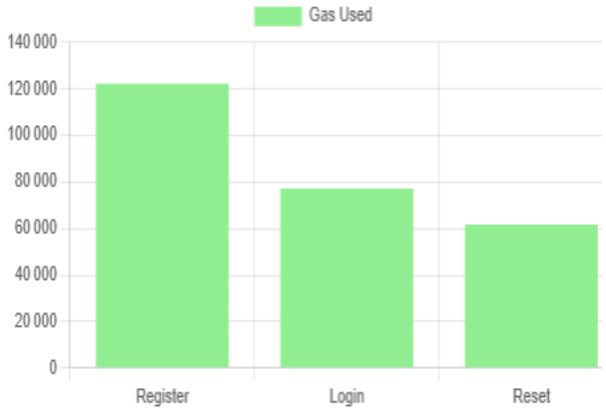

Figure 7. Average gas used vs operation

Transaction cost analysis are shown in Figure 8, calculated at an average gas price of 20 Gwei, shows that registration incurred costs of approximately 0.00024 ETH, login operations 0.00016 ETH, and password reset 0.00012 ETH. These costs demonstrate the economic feasibility of BAZKP for medical record

authentication, particularly when balanced against the enhanced security benefits.

Figure 8. Average transaction cost (ETH) vs operation

5. Discussion

This section positions the BAZKP innovation against current market standards. Through an in-depth comparative analysis against the main multifactor authentication approaches (2FA, hardware tokens, biometrics) such as [19], [25], [26], it demonstrates how our approach overcomes the limitations of traditional solutions by offering enhanced security without compromising privacy, while validating its technical and economic viability for the digital healthcare ecosystem.

Traditional 2FA systems [19] combining passwords with SMS codes or mobile tokens, while improving security over single-factor authentication, remain vulnerable to interception (e.g., SIM swapping) and centralized database breaches. BAZKP's decentralized architecture overcomes these weaknesses by eliminating vulnerable communication channels and distributing verification via blockchain.

Hardware token-based solutions [25], such as USB security keys or smart cards, are another popular choice for systems requiring enhanced security. Although they are generally considered more secure than traditional 2FA methods, they come with significant drawbacks, including cost and management challenges related to the distribution and maintenance of physical tokens. In comparison, the BAZKP mechanism does not require physical hardware while offering similar, if not superior, security through blockchain and ZKPs, thereby reducing costs and logistical complications. This digital-native approach maintains high security assurances without the physical constraints of token-based systems.

The analysis of authentication methods would be incomplete without considering biometric approaches [26], such as fingerprint and facial recognition, which also provide a high level of security but raise concerns regarding privacy and the management of sensitive biometric data, as highlighted in the literature. While BAZKP does not directly replace these solutions, it offers an interesting complement by ensuring secure authentication without exposing sensitive personal data, all while adhering to strict privacy regulations. The BAZKP mechanism's decentralized architecture and use of ZKPs create a privacy-preserving framework that prevents exposure of sensitive data while ensuring stronger security than many conventional systems.

The performance results indicate that while BAZKP introduces additional computational overhead compared to traditional authentication systems, this is justified by the significant security enhancements. The observed latencies, averaging 2-4 seconds per operation, remain within acceptable limits for medical record access scenarios where security prioritization outweighs minimal latency requirements. The gas consumption patterns align with expected blockchain resource utilization, with initial setup costs (registration) being substantially higher than subsequent authentication operations. This cost structure makes BAZKP particularly suitable for healthcare applications where user registration occurs infrequently compared to regular authentication events.

The table 2 provides a comparative analysis based on key security and usability metrics.

Table 2. Comparison of existing MFA methods

Method	Security Level	Privacy Protection	Cost	Usability
2FA [19]	Medium	Low	Low	High
Hardware Tokens [25]	High	Medium	High	Medium
Biometrics [26]	High	Low (Data Exposure)	Medium-High	High
BAZKP (Proposed)	Very High	Very High (ZKP)	Low	Medium

The findings of this research underscore the necessity for innovative solutions to tackle the evolving data security challenges faced by the healthcare sector. By replacing traditional passwords with mechanisms that only store the character count, we have demonstrated that protecting sensitive information is achievable without compromising user experience. Furthermore, the use of ZKP allows for the verification of user identity without exposing their confidential information, thereby enhancing trust in digital health systems.

6. Conclusion

In conclusion, our proposed smart contract-based multi-factor authentication mechanism represents a significant advancement in securing medical records within the digital healthcare landscape. The principal outcomes of this research are as follows:

- We have designed and implemented a novel Blockchain Authentication with Zero-Knowledge Proof (BAZKP) mechanism that successfully creates a tamper-proof and transparent environment for medical record tracking by leveraging blockchain technology and smart contracts.
- The proposed system introduces a key innovation by storing only the character count structure of passwords instead of the actual credentials, significantly mitigating the risks associated with password theft and data breaches, while integrating zero-knowledge proofs to enable secure identity verification without exposing any sensitive user information.
- Performance evaluation conducted over 100 transactions demonstrated the system's practical viability, with quantifiable metrics for latency, gas consumption, and transaction costs across core operations (registration, login, password reset), confirming its economic feasibility for healthcare applications.
- Comparative security analysis established that BAZKP provides superior privacy protection and security levels compared to conventional MFA methods like 2FA, hardware tokens, and biometrics, while avoiding their respective drawbacks in cost, usability, and data exposure.

In terms of theoretical and practical contribution, this research makes three distinct contributions to the literature: a privacy-preserving medical authentication framework through the unique character-count storage model, empirical validation of ZKP feasibility in high-security healthcare contexts, and a reference architecture for blockchain-health integration that addresses both regulatory and technical requirements.

To address the remaining challenges and opportunities, future research should should explore ZKP performance optimization for resource-constrained medical IoT devices, interoperability with other health blockchains, and emergency access protocols that preserve privacy.

Overall, this work directly addresses critical cybersecurity challenges in healthcare, ultimately enhancing trust in digital health systems by safeguarding the confidentiality, integrity, and privacy of patient information, and thereby contributing meaningfully to the sector's ongoing digital transformation.

Declarations

Author Contributions

Z.E. designed the study, conducted the research, developed the software, analyzed the data, and wrote the original manuscript. H.Z. and N.I. supervised the work, validated the methodology, and reviewed and edited the manuscript. M.E. and S.E. participated in the formal analysis. All authors have read and approved the final version of the manuscript.

Data Availability Statement

Data is contained within the article.

Funding

Not applicable.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] R. Vichayanan, K. Muhammad Saleem, A. Javed, and T. Uthen. "Blockchain-Enabled Internet of Things (IoT) Applications in Healthcare: A Systematic Review of Current Trends and Future Opportunities". International Journal of Online & Biomedical Engineering, vol. 19, no 10, 2023. https://doi.org/10.3991/ijoe.v19i10.41399

[2] A F. Alhamzah, Q N. Akhtar, K. Nohman, C. Rabia and A. Javed. "The blockchain technologies in healthcare: prospects, obstacles, and future recommendations; lessons learned from digitalization". International Journal of Online & Biomedical Engineering, vol. 18, no 09, 2022. https://doi.org/10.3991/ijoe.v18i09.32253

[3] E. Azzedine, A. Imam, T.Ayoub, B. Mohamed, H. Laamar and E. Rachid. "Proposed Architecture for Hospital 4.0: Integrating IoT, Edge AI, and Blockchain for Secure and Efficient Healthcare Systems ". International Journal of Online & Biomedical Engineering, vol. 21, no 5, 2025. https://doi.org/10.3991/ijoe.v21i05.52991

[4] B.Estefano, A.Adrian, C.Bruno, C. José Luis and W.Lenis . Interoperability Blockchain, InterPlanetary File System and Health Level 7 Framework for Electronic Health Records. International Journal of Online & Biomedical Engineering, vol. 20, no 15, 2024. https://doi.org/10.3991/ijoe.v20i15.51515

[5] F. Ahamed, F. Farid, B. Suleiman, Z. Jan, L. A. Wahsheh, and S. Shahrestani, "An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services," Future Internet, vol. 14, no 8, p. 222, July 2022,

https://doi.org/10.3390/fi14080222
[6] N. Hamed and A. Yassin, "Secure Patient Authentication Scheme in the Healthcare System Using Symmetric Encryption," Iraqi J. Electr. Electron. Eng., vol. 18, no. 1, pp. 71–81, June 2022, https://doi.org/10.37917/ijeee.18.1.9
[7] B. Sharma, R. Halder, and J. Singh, "Blockchain-based Interoperable Healthcare using Zero-Knowledge Proofs and Proxy Re-Encryption," in 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India: IEEE, pp. 1–6, Jan. 2020. https://doi.org/10.1109/COMSNETS48256.2020.9027413
[8] T. Suleski and M. Ahmed, "A Data Taxonomy for Adaptive Multifactor Authentication in the Internet of Health Care Things," J. Med. Internet Res., vol. 25, p. e44114, Aug. 2023, https://doi.org/ 10.2196/44114
[9] M. Fareed and A. A. Yassin, "Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system," Bull. Electr. Eng. Inform., vol. 11, no. 4, pp. 2131–2141, Aug. 2022. https://doi.org/10.11591/eei.v11i4.3658
[10] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare," Sensors, vol. 23, no. 21, p. 8944, Nov. 2023. https://doi.org/10.3390/s23218944
[11] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," Digit. Health, vol. 9, p. 20552076231177144, Jan. 2023. https://doi.org/10.1177/20552076231177144
[12] S. Renukappa, P. Mudiyi, S. Suresh, W. Abdalla, and C. Subbarao, "Evaluation of challenges for adoption of smart healthcare strategies," Smart Health, vol. 26, p. 100330, Dec. 2022. https://doi.org/10.1016/j.smhl.2022.100330
[13] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for Blockchain-Based IoT Systems: A Review," Appl. Sci., vol. 13, no. 13, p. 7432, June 2023. https://doi.org/10.3390/app13137432
[14] A. A. Al-saggaf, T. Sheltami, H. Alkhzaimi, and G. Ahmed, "Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing," Arab. J. Sci. Eng., vol. 48, no. 2, pp. 2347–2357, Feb. 2023. https://doi.org/10.1007/s13369-022-07235-0
[15] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment," Sensors, vol. 24, no. 11, p. 3575, June 2024. https://doi.org/10.3390/s24113575
[16] R. Bhan, R. Pamula, P. Faruki, and J. Gajrani, "Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network," J. Supercomput., vol. 79, no. 14, pp. 16233–16274, Sept. 2023. https://doi.org/10.1007/s11227-023-05272-6
[17] Regulation (EU) 2016/679 (GDPR)," European Parliament and Council, 2016. Available online: https://gdpr-info.eu/.
[18] Health Insurance Portability and Accountability Act of 1996 (HIPAA)," U.S. Congress, 1996. Available online: https://www.hhs.gov/hipaa/for-professionals/index.html.
[19] H. A. Abdulmalek and A. A. Yassin, "Secure two-factor mutual authentication scheme using shared image in medical healthcare environment," Bull. Electr. Eng. Inform., vol. 12, no. 4, pp. 2474–2483, Aug. 2023. https://doi.org/10.11591/eei.v12i4.4459
[20] V. Rajasekar, P. Jayapaul, S. Krishnamoorthi, and M. Saračević, "Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications: A Multilayer Systematic Survey," Acta Polytech. Hung., vol. 18, no. 3, pp. 87–106, 2021. https://doi.org/10.12700/APH.18.3.2021.3.5
[21] A. Ahmad and S. Jagatheswari, "Quantum Safe Multi-Factor User Authentication Protocol for Cloud-Assisted Medical IoT," IEEE Access, vol. 13, pp. 3532–3545, 2025. https://doi.org/10.1109/ACCESS.2024.3523530
[22] T. Suleski and M. Ahmed, "A Data Taxonomy for Adaptive Multifactor Authentication in the Internet of Health Care Things," J. Med. Internet Res., vol. 25, p. e44114, Aug. 2023. https://doi.org/10.2196/44114.
[23] Z. Elhadari, H. Zougagh, N. Idboufker, and M. Ech-chebaby, "Survey on the Adoption of Blockchain Technology in Internet of Things Environments: Techniques, Challenges and Future Research Directions" vol. 52, no. 1, 2025. Available online: https://www.iaeng.org/IJCS/issues_v52/issue_1/IJCS_52_1_08.pdf
[24] Z. Elhadari, H. Zougagh, N. Idboufker, and M. Ech-chebaby, "A Secure Data Storage Model for Wearable Medical IoT Devices Using Blockchain Technology," vol. 52, no. 7, 2025. Available online: https://www.iaeng.org/IJCS/issues_v52/issue_7/IJCS_52_7_14.pdf
[25] M. A. Khan, H. Alhakami, W. Alhakami, A. V. Shvetsov, and I. Ullah, "A Smart Card-Based Two-Factor Mutual Authentication Scheme for Efficient Deployment of an IoT-Based Telecare Medical Information System," Sensors, vol. 23, no. 12, p. 5419, June 2023. https://doi.org/10.3390/s23125419
[26] E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, "Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records," J. Sens. Actuator Netw., vol. 11, no. 4, p. 85, Dec. 2022. https://doi.org/10.3390/jsan11040085
[27] MOHAMED RIMSAN, Ahmad Kamil Mahmood. Application of blockchain and smart contract to ensure temper-proof data availability for energy supply chain.

Journal of Hunan University Natural Sciences, vol. 47, no 10, 2020. Available online: https://jonuns.com/index.php/journal/article/view/460/457
[28] NGUYEN QUOC KHANH, Ta Hoang Giang. Blockchain: The Driving Force behind the World's Post-COVID-19 Economy. Journal of Hunan University Natural Sciences, vol. 49, no 1, 2022. https://doi.org/10.55463/issn.1674-2974.49.1.8

参考文:

[1] R. Vichayanan、K. Muhammad Saleem、A. Javed 和 T. Uthen. 《基于区块链的医疗物联网应用：当前趋势与未来机遇系统综述》·《在线与生物医学工程国际期刊》，第 19 卷第 10 期，2023 年. https://doi.org/10.3991/ijoe.v19i10.41399
[2] A F. Alhamzah、Q N. Akhtar、K. Nohman、C. Rabia 和 A. Javed. 《医疗健康领域的区块链技术：前景、障碍与未来建议——数字化经验教训》·《在线与生物医学工程国际期刊》，第 18 卷第 09 期，2022 年. https://doi.org/10.3991/ijoe.v18i09.32253
[3] E. Azzedine、A. Imam、T.Ayoub、B. Mohamed、H. Laamar 和 E. Rachid. 《医院 4.0 架构提案：集成物联网、边缘人工智能和区块链构建安全高效的医疗系统》·《在线与生物医学工程国际期刊》·第 21 卷第 5 期，2025 年. https://doi.org/10.3991/ijoe.v21i05.52991
[4] B.Estefano、A.Adrian、C.Bruno、C. José Luis 和 W.Lenis. 《基于区块链、星际文件系统和 HL7 框架的电子健康记录互操作性研究》·《在线与生物医学工程国际期刊》，第 20 卷第 15 期，2024 年. https://doi.org/10.3991/ijoe.v20i15.51515
[5] F. Ahamed、F. Farid、B. Suleiman、Z. Jan、L. A. Wahsheh 和 S. Shahrestani. 《面向个性化医疗服务的智能多模态生物特征认证模型》·《未来互联网》，第 14 卷第 8 期，第 222 页，2022 年 7 月. https://doi.org/10.3390/fi14080222
[6] N. Hamed 和 A. Yassin. 《医疗系统中使用对称加密的安全患者认证方案》·《伊拉克电气与电子工程杂志》，第 18 卷第 1 期，第 71–81 页，2022 年 6 月. https://doi.org/10.37917/ijeee.18.1.9
[7] B. Sharma、R. Halder 和 J. Singh. 《基于区块链及零知识证明与代理重加密技术的互操作医疗系统》·见于《2020 通信系统与网络国际会议》，印度班加罗尔：IEEE，第 1–6 页，2020 年 1 月. https://doi.org/10.1109/COMSNETS48256.2020.9027417
[8] T. Suleski 和 M. Ahmed. 《医疗物联网中自适应多因素认证的数据分类法》·《医学互联网研究杂志》，第 25 卷，第 e44114 页，2023 年 8 月. https://doi.org/10.2196/44114
[9] M. Fareed 和 A. A. Yassin. 《电子医疗系统中保护隐私的多因素认证与基于角色的访问控制方案》·《电气工程与信息学通报》，第 11 卷第 4 期，第 2131–2141 页，2022 年 8 月. https://doi.org/10.11591/eei.v11i4.3658
[10] F. J. Jaime、A. Muñoz、F. Rodríguez-Gómez 和 A. Jerez-Calero. 《通过物联网通信安全与保护加强生物医学微机电系统中的隐私与数据安全》·《传感器》，第 23 卷第 21 期，第 8944 页，2023 年 11 月. https://doi.org/10.3390/s23218944
[11] T. Suleski、M. Ahmed、W. Yang 和 E. Wang. 《医疗物联网中的多因素认证综述》·《数字健康》，第 9 卷，第 20552076231177144 页，2023 年 1 月. https://doi.org/10.1177/20552076231177144
[12] S. Renukappa、P. Mudiyi、S. Suresh、W. Abdalla 和 C. Subbarao. 《智能医疗策略采纳面临的挑战评估》·《智能健康》，第 26 卷，第 100330 页，2022 年 12 月. https://doi.org/10.1016/j.smhl.2022.100330
[13] R. Alajlan、N. Alhumam 和 M. Frikha. 《基于区块链的物联网系统网络安全综述》·《应用科学》，第 13 卷第 13 期，第 7432 页，2023 年 6 月. https://doi.org/10.3390/app13137432
[14] A. A. Al-saggaf、T. Sheltami、H. Alkhzaimi 和 G. Ahmed. 《量子计算环境下面向物联网医疗生态系统的轻量级双因素用户认证协议》·《阿拉伯科学与工程杂志》，第 48 卷第 2 期，第 2347–2357 页，2023 年 2 月. https://doi.org/10.1007/s13369-022-07235-0
[15] S. Bamashmos、N. Chilamkurti 和 A. S. Shahraki. 《在物联网环境中使用去中心化区块链的双层多因素认证》·《传感器》，第 24 卷第 11 期，第 3575 页，2024 年 6 月. https://doi.org/10.3390/s24113575
[16] R. Bhan、R. Pamula、P. Faruki 和 J. Gajrani. 《支持区块链的、面向医疗智能手机网络信任管理的安全高效数据共享方案》·《超级计算杂志》，第 79 卷第 14 期，第 16233–16274 页，2023 年 9 月. https://doi.org/10.1007/s11227-023-05272-6
[17] 《欧盟通用数据保护条例》·欧洲议会和理事会，2016 年. 在线查阅：https://gdpr-info.eu/

[18] 《1996 年健康保险流通与责任法案》，美国国会，1996 年．在线查阅：https://www.hhs.gov/hipaa/for-professionals/index.html
[19] H. A. Abdulmalek 和 A. A. Yassin. 《医疗环境中使用共享图像的安全双因素相互认证方案》，《电气工程与信息学通报》，第 12 卷第 4 期，第 2474–2483 页，2023 年 8 月．https://doi.org/10.11591/eei.v12i4.4459
[20] V. Rajasekar、P. Jayapaul、S. Krishnamoorthi 和 M. Saračević. 《医疗保健、物联网及云应用中的安全远程用户认证方案：多层系统综述》，《匈牙利工程技术学报》，第 18 卷第 3 期，第 87–106 页，2021 年．https://doi.org/10.12700/APH.18.3.2021.3.5
[21] A. Ahmad 和 S. Jagatheswari. 《面向云辅助医疗物联网的抗量子多因素用户认证协议》，《IEEE Access》，第 13 卷，第 3532–3545 页，2025 年．https://doi.org/10.1109/ACCESS.2024.3523530
[22] T. Suleski 和 M. Ahmed. 《医疗物联网中自适应多因素认证的数据分类法》，《医学互联网研究杂志》，第 25 卷，第 e44114 页，2023 年 8 月．https://doi.org/10.2196/44114
[23] Z. Elhadari、H. Zougagh、N. Idboufker 和 M. Ech-chebaby. 《物联网环境中区块链技术应用综述：技术、挑战与未来研究方向》，《国际计算机科学杂志》，第 52 卷第 1 期，2025 年．在线查阅：https://www.iaeng.org/IJCS/issues_v52/issue_1/IJCS_52_1_08.pdf
[24] Z. Elhadari、H. Zougagh、N. Idboufker 和 M. Ech-chebaby. 《利用区块链技术为可穿戴医疗物联网设备构建安全数据存储模型》，《国际计算机科学杂志》，第 52 卷第 7 期，2025 年．在线查阅：https://www.iaeng.org/IJCS/issues_v52/issue_7/IJCS_52_7_14.pdf
[25] M. A. Khan、H. Alhakami、W. Alhakami、A. V. Shvetsov 和 I. Ullah. 《基于智能卡的双因素相互认证方案及其在物联网远程医疗信息系统中的高效部署》，《传感器》，第 23 卷第 12 期，第 5419 页，2023 年 6 月．https://doi.org/10.3390/s23125419
[26] E. Barka、M. Al Baqari、C. A. Kerrache 和 J. Herrera-Tapia. 《基于生物特征与区块链的保护医疗记录隐私、安全及访问控制的系统实现》，《传感器与执行器网络杂志》，第 11 卷第 4 期，第 85 页，2022 年 12 月．https://doi.org/10.3390/jsan11040085
[27] MOHAMED RIMSAN 和 Ahmad Kamil Mahmood. 《应用区块链与智能合约确保能源供应链数据可用性与防篡改性》，《湖南大学学报自然科学版》，第 47 卷第 10 期，2020 年．在线查阅：https://jonuns.com/index.php/journal/article/view/460/457
[28] NGUYEN QUOC KHANH 和 Ta Hoang Giang. 《区块链：后疫情时代世界经济的驱动力》，《湖南大学学报自然科学版》，第 49 卷第 1 期，2022 年．https://doi.org/10.55463/issn.1674-2974.49.1.8

Manuscript Information
Word count: 7,583 words (excluding references).

Peer-Review Record
Fast-track status: Not fast-tracked.
First-round reviews received: 3 reports.
Revision cycles completed: 3 rounds.
Final version submitted: January 6, 2026