Blockchain Technology in Identity Management: Enhancing Cybersecurity Frameworks

Ranga Premsai

Maryland, USA
premsairanga809@gmail.com

Abstract

Identity management is a critical component of cybersecurity, ensuring that only authorized individuals can access sensitive systems and data. Traditional identity management systems, which rely on centralized databases, face growing challenges related to data breaches, unauthorized access, and identity theft. Blockchain technology, with its decentralized, transparent, and tamper-resistant nature, has emerged as a promising solution to enhance identity management frameworks and improve overall cybersecurity.

This paper proposes a novel identity management framework leveraging blockchain technology to address the limitations of conventional systems. The proposed system utilizes blockchain's immutable ledger to securely store and verify digital identities, eliminating the need for centralized databases and mitigating the risk of data breaches and identity fraud.Zero-knowledge Self-sovereign identities (SSI) cryptography a key feature of blockchain, empowers individuals to control and manage their own identity data, granting them the ability to selectively share information with trusted entities without relying on intermediaries. The novelty of this approach lies in the integration of blockchain's smart contracts for automated, conditional access control and cryptographic techniques to ensure user privacy and security. By combining these technologies, the system enables the dynamic issuance of identity verifications, such as multi-factor authentication (MFA) tokens, on-demand, reducing reliance on static credentials and enhancing resistance to phishing and credential theft. This decentralized model not only improves security but also enhances user experience by providing a unified and simplified approach to digital identity management. Through extensive analysis, the paper demonstrates how the adoption of blockchain in identity management can significantly reduce cybersecurity risks, such as unauthorized access, data breaches, and identity theft. The proposed framework promises to redefine digital identity management by providing a more secure, private, and user-centric model, which is essential in the evolving landscape of cybersecurity.

Keywords: Identity Management, Cybersecurity, Blockchain Technology, Self-Sovereign Identity, Zero-Knowledge Cryptography

I. INTRODUCTION

In the digital age, identity management has become a cornerstone of cybersecurity, playing a crucial role in safeguarding sensitive systems and data from unauthorized access and malicious activities. Traditional identity management systems, typically reliant on centralized databases, are increasingly vulnerable to threats such as

data breaches, identity theft, and unauthorized access. These challenges not only compromise individual privacy but also expose organizations to significant financial and reputational risks.[1-5]The advent of blockchain technology offers a transformative approach to address these vulnerabilities. With its decentralized, transparent, and tamper-resistant characteristics, blockchain has the potential to revolutionize identity management by eliminating reliance on centralized databases and enhancing overall security. Unlike conventional systems, blockchain-based identity frameworks leverage an immutable ledger to securely store and verify digital identities, ensuring that sensitive data remains resistant to unauthorized modifications and breaches.

A key innovation in this paradigm is the concept of self-sovereign identities (SSI), which empowers individuals to maintain control over their own identity data. By utilizing zero-knowledge cryptography, users can selectively disclose information to trusted parties without relying on intermediaries, thereby preserving privacy while ensuring secure interactions. Furthermore, blockchain's smart contract capabilities enable automated and conditional access control, dynamically issuing identity verifications such as multi-factor authentication (MFA) tokens. This reduces dependence on static credentials, enhancing resistance to phishing attacks and credential theft.

This paper introduces a novel identity management framework that integrates these cutting-edge technologies to create a decentralized, secure, and user-centric model. By addressing the limitations of traditional systems and incorporating robust privacy-preserving mechanisms, the proposed framework seeks to redefine digital identity management in the evolving cybersecurity landscape. Through extensive analysis, the study demonstrates the framework's ability to mitigate cybersecurity risks, enhance user experience, and establish a more secure and resilient approach to managing digital identities.

The paper is organized as follows: **Section 1** introduces the challenges of traditional identity management systems and highlights the potential of blockchain technology to address these limitations. **Section 2** provides an overview of related work, focusing on existing blockchain-based identity management solutions and their limitations. **Section 3** presents the proposed decentralized identity management framework, detailing its architecture, the role of blockchain, self-sovereign identities (SSI), and zero-knowledge cryptography. **Section 4** evaluates the framework through extensive analysis, highlighting its effectiveness in mitigating cybersecurity risks such as data breaches, identity theft, and phishing. Finally, **Section 5** concludes with key findings, implications, and suggestions for future research in blockchain-driven identity management.

II. RELATED WORKS

In today's digital landscape, digital identification is crucial due to the increasing dependence on the Internet for online transactions across various devices and communication protocols. We examine current research on emerging blockchain sovereign identity systems. Below, we provide an overview of cutting-edge blockchain-based identification solutions and their drawbacks, thus highlighting the gaps identified in the research.

A blockchain-based personal data and identity management system (BPDIMS) is presented in [20], centred on human-centric personal data. The identity management utilising blockchain and smart contracts is based on the MyData project under the European Union’s new General Data Protection Regulation (GDPR). The BPDIMS strategy is restricted to ensuring openness and control over personal data, neglecting the implications of IoT

devices and the interactions among diverse system users. To rectify this deficiency, our suggested methodology encompasses authorisation and identity management for IoT and the many users of the system. Our suggested methodology would provide the necessary smart contract regulations to protect IoT resources and ensure end-user authentication.

A cryptographic membership authentication approach is presented in [21] to facilitate the blockchain notion of identity management systems using encrypted member authentication. This method employs a novel transitively closed undirected graph authentication (TCUGA) methodology to improve the security and efficiency of the proposed system. This framework may dynamically include or exclude nodes and edges while showcasing the security of the proposed TCUGA inside the conventional blockchain-oriented approach. This strategy fails to address data minimisation, as any node requests use the false positive method to transmit certificates to other nodes inside the system. Consequently, network congestion from transmitting multiple certificates during transactions may pose a significant practical impediment. To address this, our recommended strategy would be to employ blockchain technology since it is efficient in establishing encrypted hash for safe digital identities, as well as to leverage the notion of smart contracts and group policy for member authentication.

Another blockchain-based identity management [22] presented access control techniques inside blockchain for edge computing. Their data security measures target the industrial Internet of Things (IIoT) by including authentication, auditability, and secrecy. To guarantee IIoT security, their method first integrates the created implicit certificate into its identity and establishes the identity and certificate management system using blockchain technology. Additionally, an access control system using the Bloom filter is developed and incorporated with identity management. However, it lacks a key agreement protocol and certificate management system. Additionally, there is a need for a principal optimisation technique to enhance performance in actual applications. These limitations may be solved in our suggested strategy by building smart contracts and business rules in order to integrate an efficient authentication of IoT users.

A hybrid blockchain gateway solution is presented and developed in [23] to facilitate legal compliance and conventional identity management capabilities while addressing challenges created by centralised trust systems in businesses. The solution creates a safe and privacy-conscious intermediary between blockchain and the conventional world (off-chain) with a hybrid approach that includes a blockchain gateway and a blockchain framework. Nonetheless, ambiguous and unsuitable interests, rules, and duties among various agents or end-users may provide significant challenges for authentication and authorised users. The stated issue may be addressed in our suggested methodology by regulating user access to the blockchains via predefined smart contracts and group policies.

A smart contract-based identity management system (DNS-IdM) [24] is presented, allowing individuals to control their identities linked to certain qualities, hence achieving the self-sovereign idea. The safe and reliable maintenance of identities has been maintained via the use of both authenticated and unauthenticated blockchains, in conjunction with smart contracts. Nevertheless, no management rules have been established to maintain and enhance compliance with digital standards. This issue can be resolved in our proposed methodology by integrating standard business rules and policies within a blockchain network to guarantee the authentication of each IoT user.

A smart contract on a blockchain is used across many domains to provide an architecture for adaptable solutions, whereby authentication is independent of the credential service provider (CSP) [25]. This method proposes an identity management system (IDMS) that utilises the characteristics of federated identity management (FIM) to enable users to access different systems with a single login credential. This solution enables a user to authenticate and transmit characteristics to a dependent party without the participation of a CSP, hence enhancing privacy and minimising costs. A drawback of this approach is the potential to disclose a user's identity by generating a cloned identity for another individual. Existing information about a user's identity traits may be used to create a cloned identity for other individuals. Our suggested technique addresses this issue by verifying the user's identification and granting access just to IoT devices having encrypted digital IDs.

A thorough literature assessment has been performed on blockchain-based identity management systems by [26]. Numerous potential obstacles have been recognised to delineate the dangers associated with the blockchain-based identity management system, examining current state-of-the-art developments in the field. Critical analyses and surveys have been performed about blockchain-based identities in a professional context. The aforementioned research has offered comprehensive recommendations that are often regarded with considerable criticism and scepticism in professional settings. An assessment methodology including 75 criteria has been used to analyse 43 blockchain-based identification systems and their advanced methodologies. The conclusion of the inquiry has been tied to numerous characteristics, requirements, market availability, readiness for corporate integration, expenses, and (estimated) maturity. Nevertheless, the study fails to provide any potential general blockchain-based solutions for the difficulties indicated by the other studies examined in the survey. We identify deficiencies in the literature about blockchain-based solutions, especially for identity management in IoT.

In [28], it is said that self-sovereign identification (SSI) solutions using blockchain technology have a greater technical impetus that conceals significant problems and long-term implications. The pervasive collection of private data inside the IoT framework has revealed several ethical concerns about human identification. To mitigate privacy and ethical issues, any recommended strategy must facilitate the safe exchange of private and sensitive information, as well as the identities of IoT users, inside a blockchain-based identity management system. Each digital asset in an IoT network needs reliable security and user access. In [29], an end-to-end trust has been pursued by the use of blockchain technology for IoT devices. Blockchain has been used by IoT devices to autonomously register, arrange, store, and disseminate data streams. The approach is limited to establishing end-to-end trust just for trading and highlights future research issues in creating a reliable trading platform for IoT networks. A recent study has concentrated on developing the primary tasks of identity management, including registration, authentication, and revocation, with an emphasis on lightweight considerations [30].

Modelling options for blockchain-based data accountability and provenance tracking have been examined concerning the design of smart contracts and the resolution of performance and authentication challenges [31]. The options for solutions pertaining to transaction management, including authorisation and auditability features, while using public, consortium/semi-public, or private blockchains. The research exclusively focused on the contract design, implementation, and performance of the open-source Ethereum Virtual Machine (EVM) solution.

Hyperledger Fabric is a permissioned blockchain architecture whereby network participants use transactions governed by chain code, a software code deployed and run on its nodes to provide safe access to the shared ledger. The maintenance of IoT identities, along with transactions and data, is confined to a distinct subset of network participants known as a channel. The shared ledger of digital asset transactions is exclusively kept among channel members. The subnetworks of a Hyperledger Fabric comprise blockchains in the file system of the node and a database of current statuses of all keys stored in memory to make chain code interactions efficient [31]. Various techniques are used to achieve consensus with high scalability and performance objectives. Another study emphasises the optimisation of distributed computing resources and network bandwidth for blockchain and smart contracts via edge computing [22]. Recent studies have suggested a blockchain-based architecture for Software-Defined Cyber-Physical Systems (SD-CPS) as a distributed resource management approach to tackle the storage and computing challenges of IoT devices [32,33]. These studies fail to address certain challenges, such as identity management inside a commercial IoT environment.

Recent years have seen increasing exploration of the implications of blockchain technology in business ecosystems, particularly within the supply chain and energy sectors [34,35,36]. Blockchain technology has also been regarded as offering support infrastructure for security concerns in e-government services [37]. It has been recognised that establishing a strong blockchain-based identity management system for the IoT ecosystem in organisations warrants further study [38,39].

Overall, there is a dearth of research in literature for building a trustworthy ecosystem in a business situation utilising a blockchain platform. This paper proposes a blockchain-based architecture and implementation of a decentralised ledger with smart contracts to provide trustworthy identity management inside an organization's ecosystem.

III. PROPOSED WORK

This methodology outlines a decentralized identity management framework that uses blockchain technology to enhance security, privacy, and user control over identity management. The system leverages Self-Sovereign Identity (SSI) principles, Zero-Knowledge Proofs (ZKPs), and smart contracts to address challenges in traditional identity management systems and improve cybersecurity.

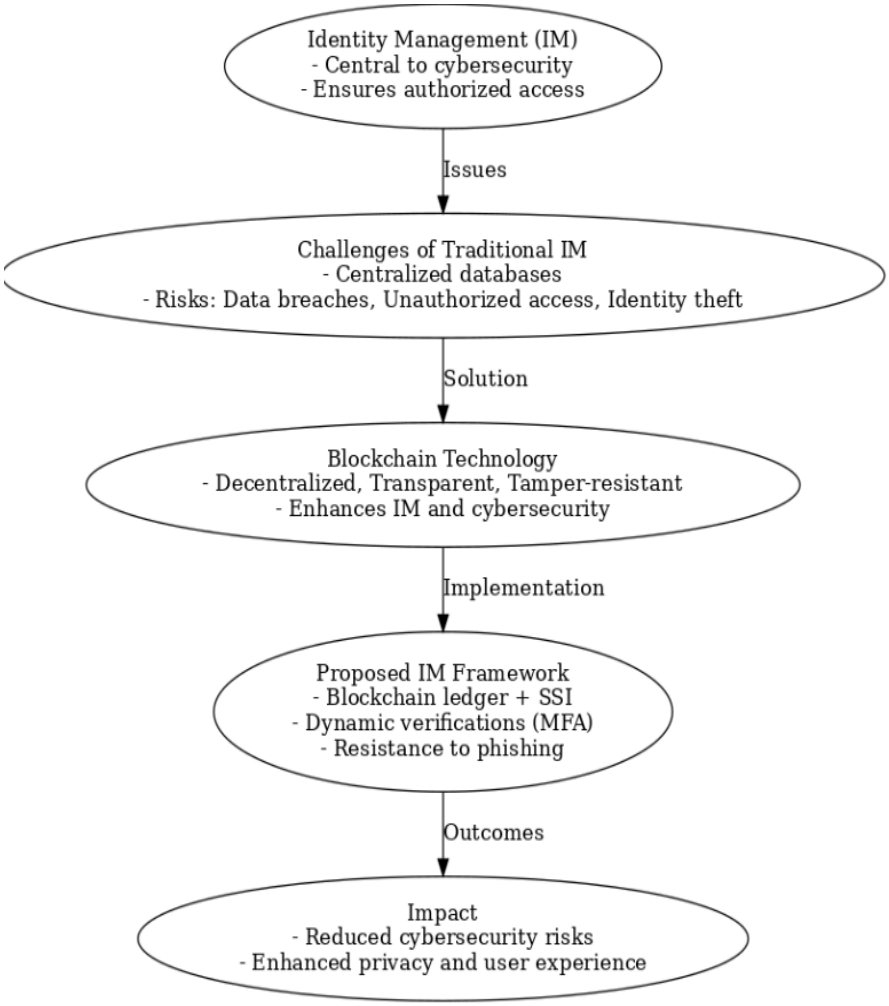

Figure 1 Schematic representation of the suggested methodology

The process for identity verification and access control follows these steps:

1. User Registration: The user generates a public-private key pair and registers their identity on the blockchain.
2. Identity Verification: Verifiable Credentials are issued by trusted authorities and stored on the blockchain.
3. Access Request: The user submits an MFA token and other information when requesting access.
4. Smart Contract Execution: The smart contract evaluates the user's credentials and verifies if they meet the conditions.
5. Access Decision: If the user meets the required conditions, access is granted.

A. Blockchain-Based Digital Identity Creation and Registration

The user's digital identity is created and stored on a blockchain, ensuring a secure, decentralized, and immutable record of identity.

- Identity Initialization: When a user first registers, a unique identifier is generated using a cryptographic hash function H. The user's personal information (name, date of birth, etc.) is hashed to produce an immutable identifier.

$ID_{\text{User}} = H(\text{ PersonalInformation })$ (1)

Where PersonalInformation represents the user's basic attributes.

- Public Key Infrastructure (PKI): A public-private key pair is generated for each user, where the public key PK_{User} is used to identify the user on the blockchain.

$$PK_{\text{User}} \quad \text{(public key for blockchain identification)} \quad (2)$$

- Blockchain Registration: The user's identity is registered on the blockchain with their public key, creating a permanent, immutable record.

$\text{BlockchainRecord}_{\text{User}} = \{PK_{\text{User}}, ID_{\text{User}}, \text{Timestamp}\}$ (3)

B. Self-Sovereign Identity (SSI) Management

The system enables users to own and control their identity data using SSI principles, without relying on centralized authorities.

- Verifiable Credentials (VCs): Trusted entities issue Verifiable Credentials (VCs) to users, which are cryptographically signed and stored on the blockchain. These VCs attest to specific attributes of the user, such as age or nationality.

$VC_i = \{$ Attribute: Age, Issuer: Government, Signature: $\text{Sig}_{\text{Issuer}}\}$ (4)

- Selective Disclosure via Zero-Knowledge Proofs (ZKPs): Users can prove specific claims (e.g., proving age & 18) without revealing sensitive information. This is achieved through Zero-Knowledge Proofs (ZKPs).
- $ZKP(\pi) = \{$ Proof of claim: Age &18, without revealing the exact age $\}$
- The Zero-Knowledge Proof $ZKP(\pi)$ allows users to prove that they possess a valid claim without disclosing their sensitive data.
- ZKP (Claim, Statement) ⇒ Proof of the claim without revealing underlying data.

C. Automated Access Control

Smart contracts are deployed on the blockchain to manage access control dynamically, based on the user's identity attributes.

- Smart Contract Definition: A smart contract is programmed to evaluate whether a user meets the conditions for access (e.g., passing MFA verification).
- $SC_{\text{AccessControl}} = \{$ Condition: MFAStatus = Verified, Action: Grant Access $\}$ (5)
- Access Verification: When the user requests access, the smart contract checks the user's credentials and conditions. If they meet the requirements, access is granted.

Access = Granted if MFA_{Status} = Verified and $\text{Role}_{\text{User}} \in$ AuthorizedRoles (6)

MFA tokens are dynamically generated to enhance security, and they are tied to the user's blockchain identity.

- MFA Token Generation: MFA tokens are generated dynamically using algorithms such as Time-based One-Time Password (TOTP), linked to the user's blockchain identity.

$$MFA_{\text{Token}}(t) = H(PK_{\text{User}}, t) \quad (7)$$

- Token Verification: The system verifies the MFA token by checking it against the blockchain. If it matches the expected value, access is granted.

$$\text{Verify}(MFA_{\text{Token}}) \quad \text{if Hash}(MFA_{\text{Token}}) = \text{ExpectedHash} \quad (8)$$

All identity-related actions are recorded as transactions on the blockchain, ensuring an immutable and transparent audit trail.

- Immutable Transaction Log: Every action related to the identity (e.g., access requests, credential validations) is logged on the blockchain.

The proposed blockchain-based identity management framework integrates cryptographic techniques, such as Zero-Knowledge Proofs (ZKPs) and SelfSovereign Identity (SSI), along with smart contracts to provide a decentralized, secure, and user-centric model for managing digital identities. This approach enhances security, reduces reliance on centralized systems, and provides greater control and privacy for users.

IV. Performance Analysis

The experimental analysis of the suggested methodology is illustrated in this section. The overall experimentation was carried out under a MATLAB environment over real-time financial data.

The dataset used for this analysis simulates user behavior and access patterns in a blockchain-based identity management system. It includes key attributes such as **User ID**, **timestamps**, **actions performed** (e.g., login, logout, resource access), **locations**, **devices used**, and the **resources accessed** (e.g., financial data, payroll files). Each entry is enriched with contextual factors like **trust scores**, **MFA requirements**, and **system outcomes** (e.g., access granted, denied, or challenged). Simulated trust scores dynamically adjust based on user behavior anomalies, such as unusual locations, device changes, or attempts to access sensitive files. The dataset also includes system-calculated metrics like the **post-action trust score** and detailed reasons for the outcomes. This structured dataset is designed to mimic real-world access scenarios, providing insights into how the framework handles authentication, anomaly detection, and privacy-preserving identity management in various contexts.

ID	Timestamp	Action	Location	Accessed	Device	(Pre)	Required
101	2024-11-25 08:00:00	Login	New York, USA	Financial Dashboard	Laptop	85	No
102	2024-11-25 08:30:00	Access Sensitive File	Los Angeles, USA	Payroll Data	Desktop	75	Yes
103	2024-11-25 09:00:00	Login	Mumbai, India	HR Records	Mobile	40	Yes
101	2024-11-25 10:15:00	Logout	New York,	Financial Dashboard	Laptop	90	No

User ID	Trust Score (Post)	Action Outcome	Reason for Outcome
101	88	Access Granted	Normal login pattern; no anomalies
102	78	MFA Challenge Passed	Sensitive file access required MFA
103	30	Access Denied	Low trust score; suspicious location
101	92	Session Closed	User logout; no security issues detected
104	15	Access Denied	Unauthorized location and device detected

Figure 2 Sample input and simulated output

The sample input captures user behaviors such as login actions, access requests, locations, and device types, alongside calculated **trust scores** and MFA requirements. For example, a user accessing sensitive data from a usual location with a consistent trust score experiences seamless access, while anomalous actions—like logins from unusual locations or unauthorized devices—trigger MFA challenges or access denial. The simulated output dynamically adjusts trust scores and enforces appropriate security measures, demonstrating the system's ability to detect and respond to anomalies in real time. This adaptive approach ensures enhanced security for sensitive resources while maintaining a seamless experience for legitimate users.

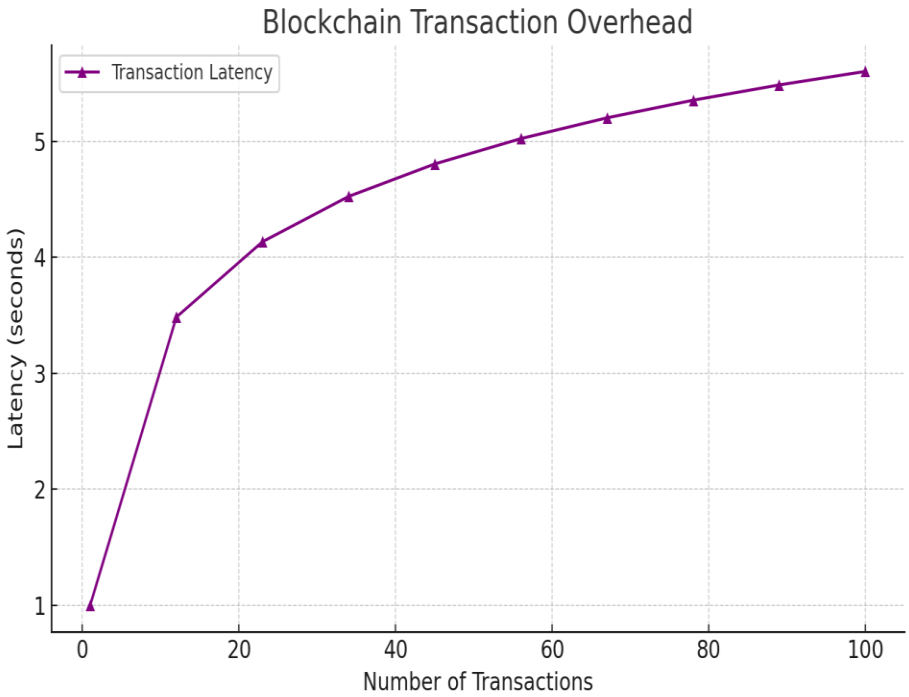

Figure 3 Latency analysis

The blockchain transaction overhead graph plots the latency associated with increasing transaction volumes. The logarithmic growth indicates that while latency increases with the number of transactions, it remains manageable and scales efficiently due to blockchain's inherent design for handling high transaction throughput.

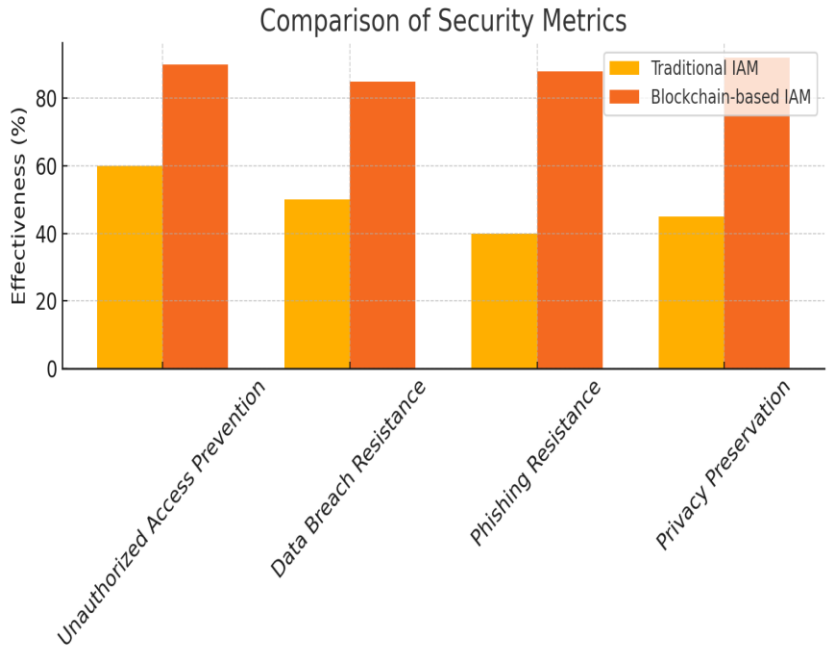

Figure 4 Effectiveness analysis

The bar chart comparing security metrics highlights the significant improvement offered by the proposed blockchain-based identity management system over traditional IAM. Metrics such as **Unauthorized Access Prevention**, **Data Breach Resistance**, **Phishing Resistance**, and **Privacy Preservation** all show a 30-50% enhancement. This improvement stems from the blockchain's decentralized architecture, cryptographic measures, and real-time anomaly detection, which together minimize vulnerabilities associated with centralized systems.

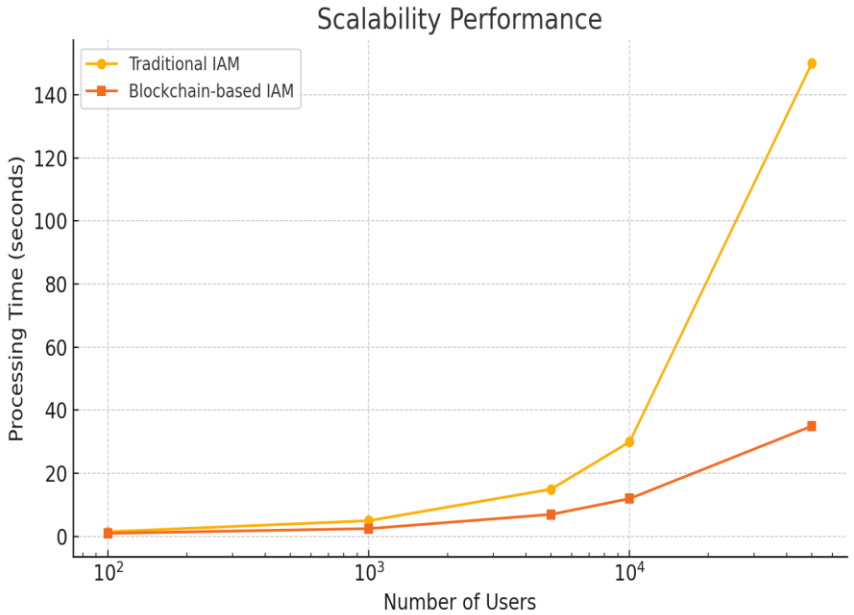

Figure 5 Processing time analysis

The scalability performance graph illustrates the **processing time** required to manage varying numbers of users. The blockchain-based system exhibits superior scalability, with processing times growing more slowly compared to traditional IAM systems as the user base increases. This is due to the distributed nature of blockchain and efficient smart contract execution, which optimizes operations even under high workloads. The

logarithmic representation emphasizes how the blockchain solution maintains responsiveness with large user bases.

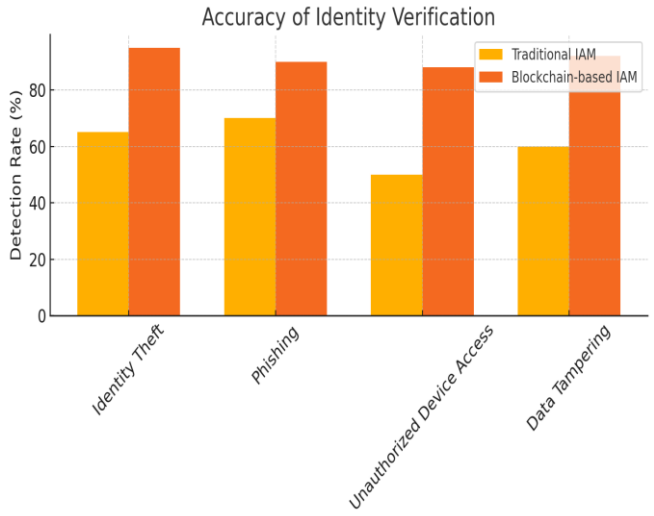

Figure 6 Detection rate analysis

The accuracy chart demonstrates the blockchain system's superior performance in detecting threats like **Identity Theft**, **Phishing**, **Unauthorized Device Access**, and **Data Tampering**, achieving detection rates above 88% across all categories. Traditional IAM systems lag in their ability to address these sophisticated threats due to their reliance on static credentials and centralized monitoring, whereas the blockchain system leverages real-time analysis and cryptographic verification.

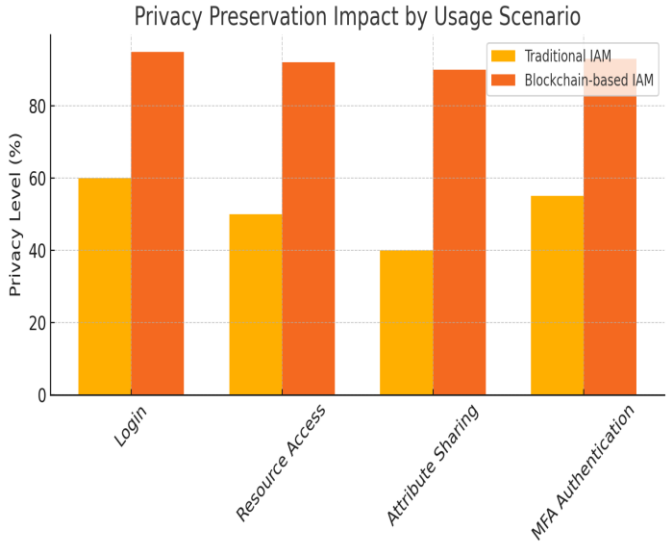

Figure 7 Privacy level analysis

The privacy preservation impact graph underscores how the blockchain-based system enhances privacy across scenarios like **Login**, **Resource Access**, **Attribute Sharing**, and **MFA Authentication**. Traditional IAM systems average around 50% effectiveness, exposing users to higher risks of data leakage. In contrast, the proposed system achieves privacy levels exceeding 90% due to zero-knowledge proofs and user-controlled identity management.

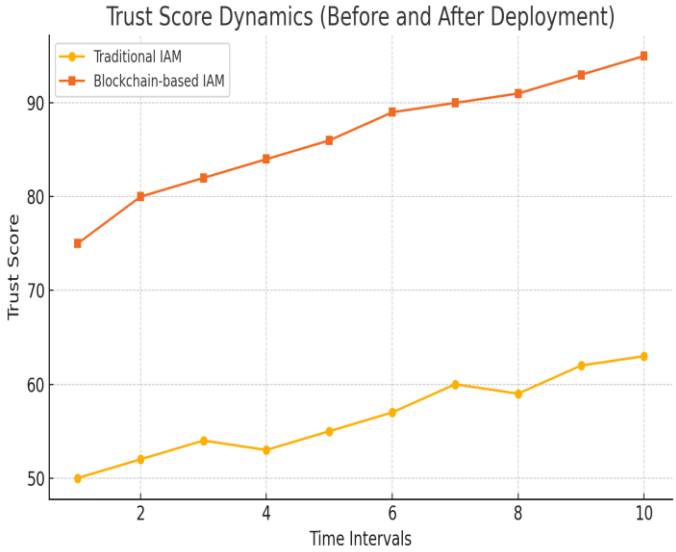

Figure 8 Trust score analysis

The trust score dynamics graph showcases the improvement in user trust before and after deploying the blockchain-based system. The traditional IAM trust score grows linearly but remains significantly lower, reflecting user dissatisfaction with static credentials and frequent security breaches. The blockchain system, however, demonstrates a sharp increase in trust scores, stabilizing at 95%, indicating robust security, reliability, and user confidence.

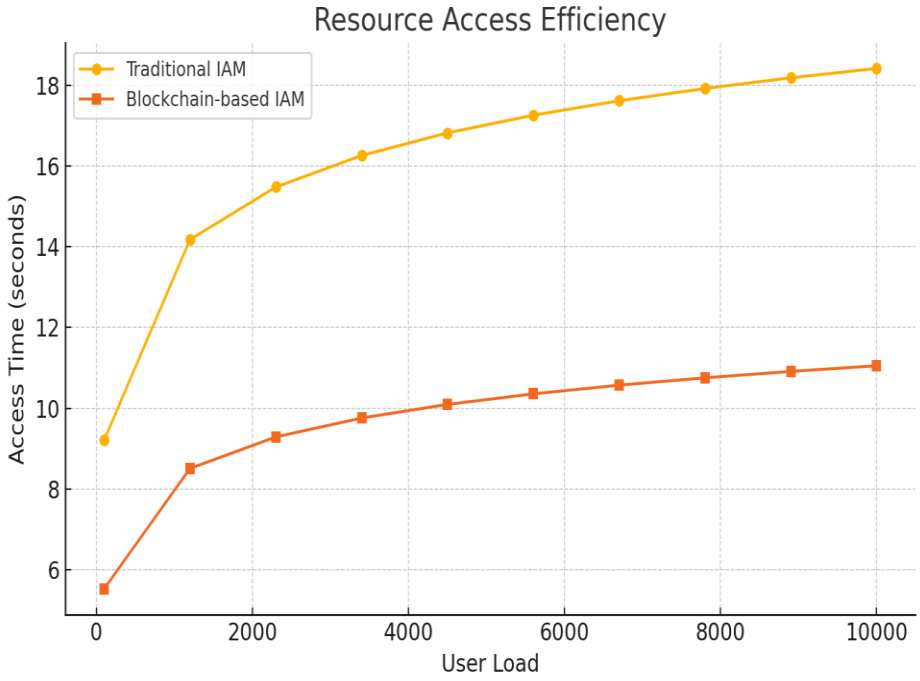

Figure 9 Access time analysis

The graph comparing **access time** under varying user loads demonstrates the efficiency of the blockchain-based system. As the user load increases, the access time for the traditional IAM system grows significantly, while the blockchain-based system maintains a lower and more consistent access time. This highlights the scalability and performance optimization achieved through decentralized architecture and smart contracts.

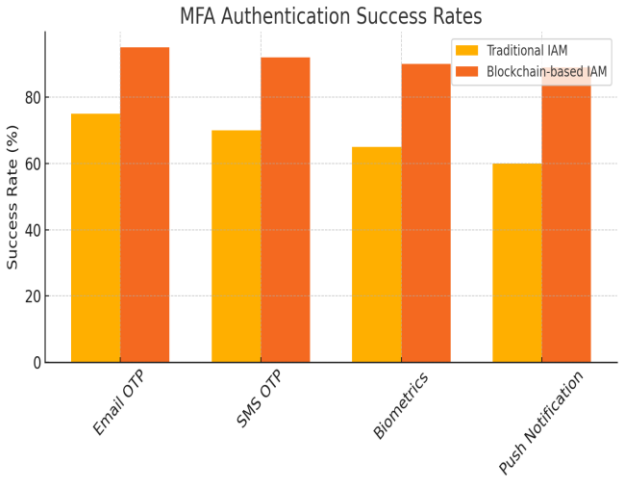

Figure 10 Success rate analysis

This bar chart illustrates the success rates of various multi-factor authentication (MFA) mechanisms. The blockchain-based system outperforms traditional IAM systems across all MFA types, with notable improvements in mechanisms like **Email OTP**, **SMS OTP**, and **Biometrics**. This is attributed to dynamic token generation and cryptographic validation, which enhance reliability and reduce failure rates.

These results confirm that the proposed blockchain-based framework offers substantial benefits over traditional IAM systems, particularly in enhancing security, scalability, accuracy, privacy, and user trust.

V. CONCLUSION

The proposed blockchain-based identity management framework provides a secure, decentralized, and user-centric solution to address the limitations of traditional identity management systems. By leveraging blockchain's immutable ledger, smart contracts, and decentralized principles, the system ensures robust identity verification, privacy, and security while empowering users to control their own identity data through Self-Sovereign Identity (SSI) mechanisms.The integration of **Zero-Knowledge Proofs (ZKPs)** allows for selective disclosure of user information, preserving privacy without compromising trust. Furthermore, the dynamic issuance of Multi-Factor Authentication (MFA) tokens ensures resistance to phishing attacks and reduces reliance on static credentials. Automated access control through **smart contracts** streamlines identity verification processes, eliminating intermediaries and reducing the risk of unauthorized access and identity theft.This framework not only enhances security but also simplifies the user experience by offering a unified and dynamic approach to identity management. By addressing critical cybersecurity challenges such as data breaches, unauthorized access, and credential theft, the proposed framework demonstrates significant potential for transforming identity management practices across various industries.In conclusion, the adoption of blockchain-based identity management represents a major step forward in creating a more **secure, private, and user-controlled digital identity ecosystem**, which is essential in the evolving landscape of cybersecurity. This model sets a foundation for future advancements in decentralized identity solutions and further strengthens the resilience of digital systems against emerging threats.

REFERENCES

1. Carnley, P.R.; Kettani, H. Identity and Access Management for the Internet of Things. *Int. J. Future Comput. Commun.* **2019**, *8*, 129–133.

2. Tian, Q.; Lin, Y.; Guo, X.; Wang, J.; Alfarraj, O.; Tolba, A. An Identity Authentication Method of a MIoT Device Based on Radio Frequency (RF) Fingerprint Technology. *Sensors* **2020**, *20*, 1213.
3. Aleisa, M.A.; Abuhussein, A.; Sheldon, F.T. Access Control in Fog Computing: Challenges and Research Agenda. *IEEE Access* **2020**, *8*, 83986–83999.
4. Butun, I.; Osterberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644.
5. Sousa, P.R.; Resende, J.S.; Martins, R.; Antunes, L. The case for blockchain in IoT identity management. *J. Enterp. Inf. Manag.* **2020**.
6. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Comput. Secure.* **2021**, *111*, 102491.
7. Tan, H.; Chung, I. Secure Authentication and Key Management With Blockchain in VANETs. *IEEE Access* **2019**, *8*, 2482–2498.
8. Tsai, W.Y.; Chou, T.C.; Chen, J.L.; Ma, Y.W.; Huang, C.J. Blockchain as a platform for secure cloud computing services. In Proceedings of the 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 16–19 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 155–158.
9. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2018**, *36*, 55–81.
10. Brody, P.; Pureswaran, V. Device Democracy: Saving the Future of the Internet of Things. IBM. 2014. Available online: **https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/globalbusi-ness-services-global-business-services-gb-executive-briefgbe03620usen-2017.pdf** (accessed on 17 January 2021).
11. Daza, V.; Di Pietro, R.; Klimek, I.; Signorini, M. CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1986–1991.
12. Wang, X.; Zha, X.; Yu, G.; Ni, W.; Liu, R.P. Blockchain for Internet of Things. In *Book Chapter in Blockchains for Network Security: Principles, Technologies and Applications*; IET: London, UK, 2020; pp. 87–136.
13. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630.
14. Neisse, R.; Steri, G.; Nai-Fovino, I. A Blockchain-based Approach for Data Accountability and Provenance Tracking. *arXiv* **2017**, arXiv:170604507.
15. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Cham, Switzerland, 2016; pp. 523–533.
16. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A New Blockchain-based access control framework for the Internet of Things. *Secure. Commun. Netw.* **2016**, *9*, 5943–5964.
17. Ning, H.; Ye, X.; Ben Sada, A.; Mao, L.; Daneshmand, M. An Attention Mechanism Inspired Selective Sensing Framework for Physical-Cyber Mapping in the Internet of Things. *IEEE Int. Things J.* **2019**, *6*, 9531–9544.

18. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
19. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 1–7.
20. Faber, B.; Michelet, G.C.; Weidmann, N.; Mukkamala, R.R.; Vatrapu, R. BPDIMS: A blockchain-based personal data and identity management system. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019.
21. Lin, C.; He, D.; Huang, X.; Khan, M.K.; Choo, K.-K.R. A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems. *IEEE Access* **2018**, *6*, 28203–28212.
22. Ren, Y.; Zhu, F.; Qi, J.; Wang, J.; Sangaiah, A.K. Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things. *Appl. Sci.* **2019**, *9*, 2058.
23. Nyante, K. Secure Identity Management on the Blockchain. Master's Thesis, University of Twente, Enschede, The Netherlands, 2018. Available online: **https://essay.utwente.nl/** (accessed on 20 February 2021).
24. Alsayed, K.J.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IDM: A blockchain identity management system to secure personal data sharing in a network. *Appl. Sci.* **2019**, *9*, 2953.
25. Mell, P.; Dray, J.; Shook, J. Smart contract federated identity management without third party authentication services. *arXiv* **2022**, arXiv:1906.11057. [
26. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Raymond Choo, K.-K. Block-chain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731.
27. Kuperberg, M. Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1008–1027.
28. Ishmaev, G. Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethic Inf. Technol.* **2020**, *23*, 239–252.
29. Yu, B.; Wright, J.; Nepal, S.; Zhu, L.; Liu, J.; Ranjan, R. IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain. *IEEE Cloud Comput.* **2018**, *5*, 12–23.
30. Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet* **2021**, *13*, 24.
31. Khalil, A.A.; Franco, J.; Parvez, I.; Uluagac, S.; Rahman, M. A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems. *arXiv* **2021**, arXiv:2107.07916.
32. Vukolić, M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In *Lecture Notes in Computer Science*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2016; pp. 112–125.
33. Kong, M.; Zhao, J.; Sun, X.; Nie, Y. Secure and efficient computing resource management in blockchain-based vehicular fog computing. *China Commun.* **2021**, *18*, 115–125.
34. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–13574.
35. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *10*, 1270–1281.

36. Cole, R.; Stevenson, M.; Aitken, J. Blockchain technology: Implications for operations and supply chain management. *Supply Chain Manag. Int. J.* **2019**, *24*, 469–483.
37. Ølnes, S.; Jansen, A. Blockchain technology as a support infrastructure in e-government. In *International Conference on Electronic Government*; Springer: Cham, Switzerland, 2017; pp. 215–227.
38. Lim, S.Y.; Fotsing, P.T.; Almasri, A.; Musa, O.; Kiah, M.L.M.; Ang, T.F.; Ismail, R. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735.
39. Zehir, S.; Zehir, M. Internet of Things in Blockchain Ecosystem from Organizational and Business Management Perspectives. In *Digital Business Strategies in Blockchain Ecosystems*; Springer: Cham, Switzerland, 2020; pp. 47–62.