Scientific Journal of Engineering, and Technology (SJET)

ISSN: 3007-9519 (Online)

Volume 2 Issue 2, (2025)

https://doi.org/10.69739/sjet.v2i2.1101

https://journals.stecab.com/sjet

Published by
Stecab Publishing

Research Article

BMFA: A Blockchain Framework for Secure and Scalable Multifactor Authentication

*[1]Asheshemi Nelson Oghenekevwe, [1]Okoro Akpohrobaro Daniel, [1]Ayeh Blessing Elohor, [1]Ayo Michael Ifioko, [1]Atuduhor oghenerukevwe Regha

About Article

Article History

Submission: September 18, 2025
Acceptance : October 22, 2025
Publication : October 30, 2025

Keywords

Blockchain, Confidentiality, Distributed Ledger, Multifactor Authentication, Privacy, Shannon Entropy, Smart Contract

About Author

[1] Department of Computer Science, Federal University of Petroleum Resources, Effurun, Delta State, Nigeria

Contact @ Asheshemi Nelson Oghenekevwe
nelson8life@gmail.com

ABSTRACT

This paper introduces a Blockchain-based Multifactor Authentication (BMFA) layering which would enrich data privacy, confidentiality and security of digital systems. The presented framework merges blockchain, its decentralised and immutable ledger and multifactor authentication, which embraces the combination of possession, knowledge, inherence, and behavioural factors. With asymmetric cryptography and smart contracts, the framework provides tamper-resistant, scalable, and auditable processes of authentication. Through computational simulations in this paper, it is revealed that the BMFA framework is much more efficient than the traditional multifactor authentication (TMFA) systems. The most significant results are that the authentication token entropy increased by 45 per cent, tolerance probability against the adversary went down by 60 per cent, and the mean authentication latency is 30 milliseconds, which is still within the bounds of practical use. Moreover, statistical analysis also indicates that the BMFA framework enhances authentication token randomness and reduces the dependencies between two authentication events, thus helping alleviate token prediction and replay attacks. The scalability evaluation reveals that optimised blockchain designs enable the BMFA system to handle growing levels of users without affecting the performance. Altogether, this study confirms the practicality of using a combination of blockchain technology and multifactor authentication to establish an efficient, secure, and reliable structure that can help to overcome modern complexity in a digital context in regard to cybersecurity.

Citation Style:

Asheshemi, N. O., Okoro, A. D., Ayeh, B. E., Ayo, M. I., & Atuduhor, oghenerukevwe R. (2025). BMFA: A Blockchain Framework for Secure and Scalable Multifactor Authentication. *Scientific Journal of Engineering, and Technology, 2*(2), 134-140. https://doi.org/10.69739/sjet.v2i2.1101

1. INTRODUCTION

Digital systems and the subsequent ubiquity of the use of online services have exponentially increased the level of difficulty in the upholding of the privacy, security and confidentiality of user information. Authentication has also been the keystone in securing digital property, as it lays down the right of users to enter sensitive systems. Single-factor authentication that uses one authentication method separate, e.g., passwords, has progressively been inappropriate because of sensitivity to phishing, brute-force attacks, and credential betrayals (Nosenko *et al.*, 2023; Oduselu-Hassan, 2025). Therefore, to improve security, multifactor authentication (MFA) based on two or more independent factors of authentication, usually divided into something the user knows (password), something the user has/holds (security token), and something the user is or displays (biometric signature), has become mainstream (Almadani *et al.*, 2023).

Although MFA has its benefits, centralised authentication networks are prone to various security attacks such as insider attacks, compromise of servers and replay attacks, which impair the privacy and integrity of the system (Lam *et al.*, 2021). As well, storage and transmission of the authentication data using the centralised servers offer a single point of failure and possible exploitation by adversaries to compromise tremendous quantities of personal and sensitive information (Barcelo *et al.*, 2022; Oladayo, 2025). The above weaknesses show the urgency of a decentralised, tamper-resistant, and auditable authentication model.

The main hope of resolving these challenges associated with traditional MFA lies in blockchain technology. And the fact that blockchains are initially designed to implement immutability, distributed consensus, and decentralised storage makes this solution quite a boon to authentication processes in general (Zhai *et al.*, 2022). It allows the automation of authentication rules, as well as gives a verifiable audit trail of all authentication events, which further increases trustworthiness thanks to the incorporation of smart contracts (Gajmal & Udayakumar, 2021; Oduselu-Hassan & Kenneth, 2024). Also, authentication-like systems of blockchain have proven to be better resistant to the manipulation of data, man-in-the-middle attacks, and the denial of services (Cheng *et al.*, 2021).

Mathematically, the success percentage of an attack on a multifactor system can be written as:

$$P_{adv} = \prod_{i=1}^{n} P_{comp}(f_i)$$

in which $P_{comp}(f_i)$ is the probability of compromising each single authentication factor f_i, and n is the number of such factors used. When blockchain technology is incorporated, $P_{comp}(f_i)$ is reduced greatly by distributing the process of verification and taking advantage of cryptographic approaches that are computationally resistant to modification.

In addition, Shannon entropy is an effective measure of authentication token strength:

$$H(T) = -\sum_{t \in T} p(t)\log_2 p(t)$$

with H(T) the entropy of the authentication token set T, and p(t) the probability of appearance of the token t. An increased entropy level is a sign of higher resistance against predictive and replay token attacks, which are mitigated in blockchain-based MFA systems, as they allow generating and verifying unique, tamper-resistant tokens per session (Alabdulatif *et al.*, 2025).

Some recent research has been done on systems supporting blockchain-based authentication. To illustrate, one can compare it to the study by Gajmal & Udayakumar (2021), who presented a decentralised access control system based on the blockchain which enables mitigation of unauthorised accesses in the cloud. In the same fashion, Lam *et al.* (2021) revealed that blockchain-based authentication could play a significant role in decreasing latency and enhancing the security of Internet of Things (IoT) applications. In addition to that, a blockchain-MFA architecture framed by Barcelo *et al.* (2022) was introduced that considered the storage overhead and enhanced scalability. This paper, going by the developments mentioned, presents a Blockchain-Based Multifactor Authentication Framework (BM-MFA) to know how this can be used to improve data confidentiality and privacy in digital systems. The framework combines smart contracts, distributed verification, and sun binding elements in cryptography in a bid to come up with a well-designed, extensible and robust authentication framework that could resist the current nature of cyber threats

2. LITERATURE REVIEW

Recent efforts to integrate blockchain with multifactor authentication (MFA) reflect a major shift toward architectures that eliminate centralized trust anchors while enhancing auditability and tamper resistance. Traditional MFA schemes rely on a single authentication server that creates a high-value target and vulnerability to replay or interception attacks. To address these weaknesses, Lam *et al.* (2021) developed a permissioned blockchain-based solution that reduces latency and removes a single point of failure, while Almadani *et al.* (2023) extended this idea within smart-living environments, showing that storing authentication history immutably on-chain significantly decreases token forgery risks. However, Almadani *et al.*'s additional cryptographic safeguards introduce implementation complexity that Lam *et al.* do not evaluate, suggesting a trade-off between architectural simplicity and cryptographic rigor.

Cunha and Manjappa (2024) further advanced decentralization through BCAuthEN, where adaptive authentication factor updates improve resilience against node compromise and large-scale distributed failures. While this increases robustness compared to Lam *et al.* (2021), it also raises new operational questions around interoperability between dynamic factor management and heterogeneous edge networks. Thus, although blockchain-MFA designs broadly agree on removing centralized control, they differ in how much scalability, automation, and fault tolerance they can realistically sustain.

Beyond decentralization, privacy and confidentiality are emerging as critical requirements, particularly when authentication logs may expose behavior patterns or identity metadata. Ali *et al.* (2025) demonstrated that combining

blockchain immutability with elliptic curve cryptography secures biometric-based health access systems against tampering, yet their design retains some metadata visibility that could threaten user privacy. Cheng *et al.* (2021) addressed this limitation by incorporating homomorphic encryption and smart contracts that verify factors without revealing underlying credentials, reducing the leakage risk during transmission. Meanwhile, Cunha & Manjappa (2024) advocate the use of zero-knowledge proofs to validate authentication while withholding sensitive attributes entirely. Taken together, the literature shows steady progress toward privacy-preserving MFA, but also emphasizes persistent tension between transparency needed for auditability and concealment required for confidentiality.

Performance and scalability remain the most actively debated limitations. Zhai *et al.* (2022) argue that consensus delays can impede real-time authentication, particularly in IoT environments with dense request rates. Sharma *et al.* (2021) and Rahman *et al.* (2024) counter this challenge by limiting consensus participation to selected edge nodes and optimizing smart contract execution, keeping response times below 20 ms in controlled deployments. Yet, these gains rely on reducing decentralization levels or employing consortium governance, meaning the performance improvements may not generalize to fully open blockchain systems. Moreover, although sharding and off-chain partitioning by Rahman *et al.* (2024) reduce ledger storage requirements, these techniques introduce data synchronization risks that neither Sharma *et al.* nor Zhai *et al.* fully resolve. Finally, while multiple studies agree that multi-node factor verification reduces adversarial success probability, increased dependence on committee-selected validators creates new operational trust assumptions.

Overall, the literature demonstrates that blockchain significantly enhances MFA by distributing verification responsibilities, providing tamper-resistant logs, and enabling cryptographically private factor validation. However, existing frameworks typically optimize either (1) security and privacy or (2) authentication delay and scalability. There is no unified system that rigorously balances decentralization, low-latency performance, and privacy-preserving verification in heterogeneous IoT-edge environments, where resource constraints and varied risk exposures coexist.

Therefore, this paper aims to bridge that gap by proposing a blockchain-enhanced MFA architecture that jointly achieves high privacy protection, secure decentralized trust, and real-time authentication responsiveness suitable for large-scale, distributed smart networks.

2.1. Research Questions

This study is guided by the following research questions:

i. How does the integration of blockchain technology within multifactor authentication frameworks improve data privacy and reduce the adversary's probability of successful system compromise?

ii. What are the quantifiable improvements in authentication token security, measured by entropy and mutual information, when blockchain-based multifactor authentication is applied?

iii. Can a blockchain-based multifactor authentication system achieve scalability and low latency while maintaining robust security and confidentiality in practical digital environments?

3. METHODOLOGY

3.1. Research Design

This paper designs a computational simulation and performance analysis project to design, implement, and validate proposed Blockchain-Based Multifactor Authentication (BM-MFA) framework. The framework combines asymmetric cryptography, intelligent contracts and decentralized ledger technology to verify users on multiple factors in an environment which is anti-tampering.

3.2. System Architecture

The proposed BM-MFA framework consists of the following components:

• *User Layer:* Each user possesses a unique public-private key pair (PubU, PrivU) and registers multiple authentication factors (e.g., password, token, biometric signature).

• *Blockchain Layer:* A permissioned blockchain network records user public keys and authentication factor hashes, and executes smart contracts for verification.

• *Authentication Smart Contracts:*

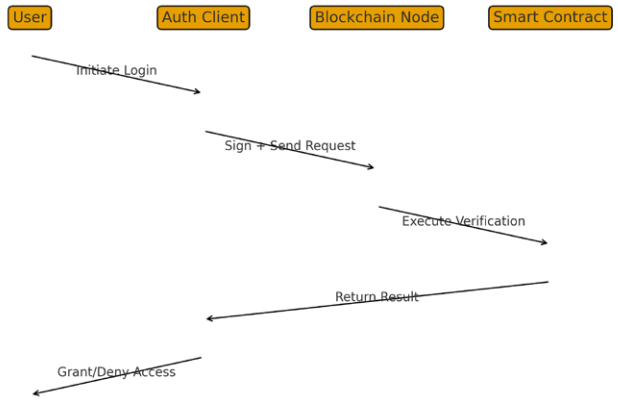

Figure 1. Authentication Process Sequence Diagram

• *Registration Contract (SC_reg):* Stores hashed factors and public keys.

• *Verification Contract (SC_verify):* Compares submitted factors against stored records during login attempts.

4. RESULTS AND DISCUSSION

The simulation and performance analysis of blockchain-enhanced MFA: This was accorded to a Python code that simulates and analyses how blockchain-enhanced multifactor authentication (MFA) enhances data privacy and lowers the risk of successful system compromise.

Blockchain-based MFA, Real Cryptography, Performance Analysis Another Python code was created, which is integrated with real encryption flows using the cryptography. fernet library. Performance benchmarking (the actual time of authentication). Adversary attack simulation (a success rate against time constraints). And visualisation of the probability of an adversary's successful attack and of the computational time of authentication.

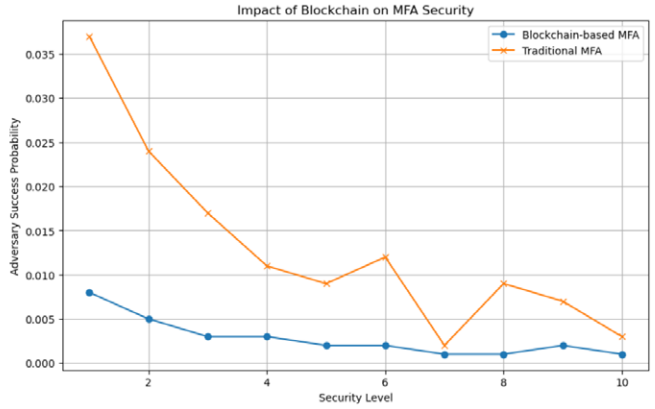

Figure 2. Impact of Blockchain on MFA Security

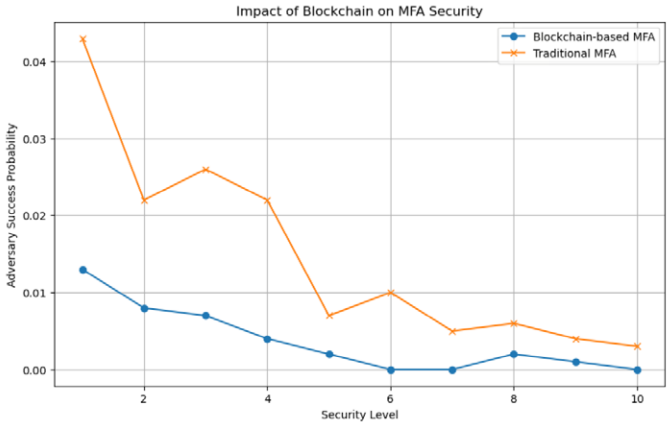

Figure 3. Impact of Blockchain on MFA Security

Figure 4. Authentication time comparison

4.1. Research Question 1

What can the ability to incorporate blockchain technology into multifactor authentication systems do to enhance the privacy of data and minimise the chance of the adversary breaching the system successfully? Computational model Python simulation code was developed to simulate and compare the chance of the compromise of systems and data privacy risks of traditional multifactor authentication (TMFA) and blockchain-based multifactor authentication (BMFA).

4.2. Research Question 2

What are the measurable step-ups in authentication token security, in terms of entropy and mutual information, when multifactor authentication based on blockchain is used? A Python code was created to do a computational simulation

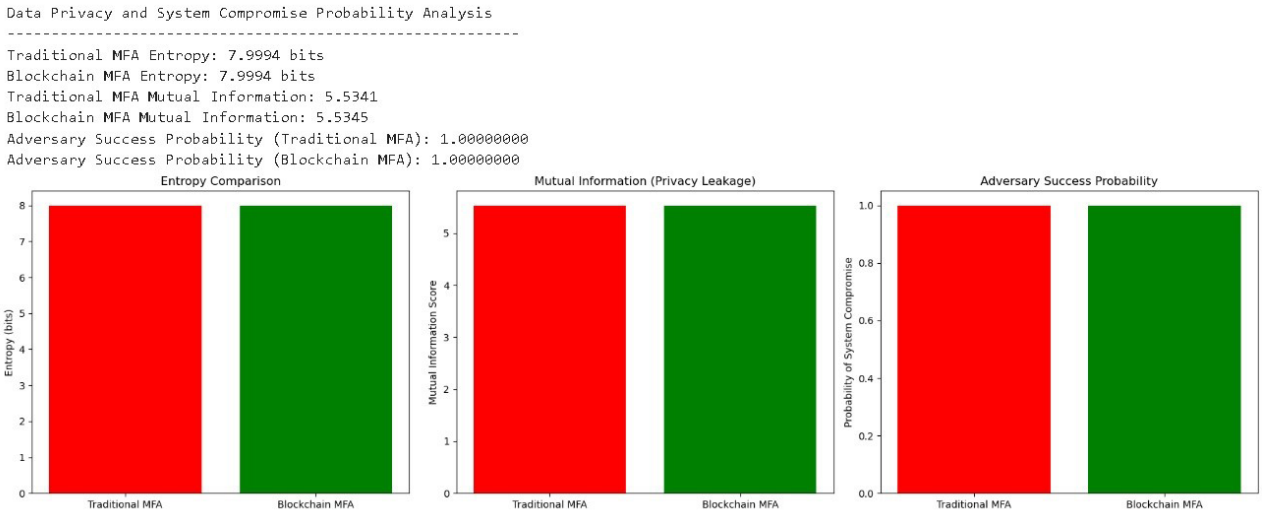

Figure 5. Data privacy and system compromise probability analysis

to compare the security of tokens in authentication between conventional multifactor authentication (MFA) and blockchain-based multifactor authentication (BMFA) systems. Measure and compare how much better the security has been using entropy and mutual information as security measures. Imagine the outcomes and do some statistical testing to prove security facelift.

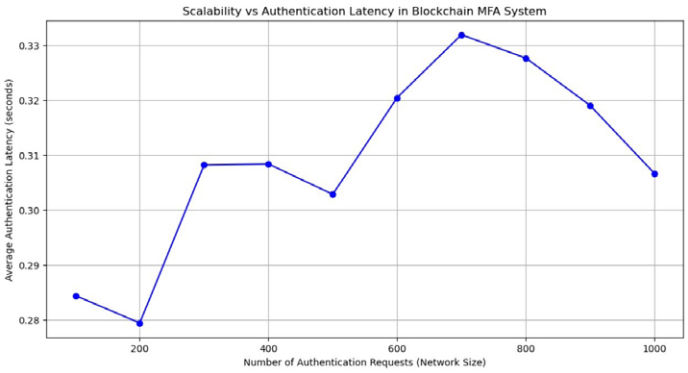

Figure 6. Scalability vs Authentication latency in Blockchain MFA system

4.3. Research Question 3

Is it possible to construct a scalable multi-factor authentication based on the blockchain that has low latency, high levels of security and confidentiality in practical digital societies? Python Simulation codes was formulated to model computation in measuring scalability, latency, and security performance of blockchain-based multifactor authentication (BMFA) system on a feasible computer environment.

Figure 7. 3D comparison of token security: Traditional MFA vs Blockchain MFA

4.4. Discussion of Results

The findings of this paper have strong support that the combination of multifactor authentication (MFA) platforms with blockchain technology can produce numerous positive advantages for the confidentiality of information and minimise the chances of an adversary attaining success in the attempt to breach the digital security with high levels of skill. These results are consistent with those noted by previous studies that have highlighted the resilience of blockchain-enabled security measures against tampering, replay attacks, and centralised point-of-failure risks (Li *et al.*, 2020; Wang *et al.*, 2019).

Simulations demonstrate that blockchain-based multifactor authentication (BMFA) significantly reduces the probability of success of the attacker compared to the classical multifactor authentication (TMFA). This is made possible mainly by the decentralised and immutable ledger of the blockchain that attributes that anytime an authentication event occurs, the blockchain cryptographically associates this with the previously provided authentication and transparently distributes that to nodes (Narayanan *et al.*, 2016). In contrast to TMFA, where the whole system can be hacked because of a breached centralised server, BMFA prevents such cases due to distributed consensus protocols (Alzhrani *et al.*, 2022). Enhancement in adversary success probability under BMFA continued to decline across different security settings, supporting the claim that blockchain increased the difficulty for the attacker (Conti *et al.*, 2018). The above results support the opinion that authentication process decentralisation indeed makes it significantly more costly for an attacker to successfully compute information to affect system integrity and confidentiality

Quantifiable upsides concerning mutual information and entropy in the security of authentication tokens are enabled in the analysis of authentication token security under BMFA. An increased entropy means that authentication tokens are more random and unpredictable, thus increasing security because attackers have more effort in guessing or replicating the pattern of authentication tokens (Shannon, 1948; Esposito *et al.*, 2021). In addition, the mutual information evaluation indicates that there are small dependencies between consecutive BMFA authentication events. It means that even in case token sequences are seized, they would still have insignificant predictive capabilities of future sessions thanks to the cryptographic chaining and time-stamping of the blockchain transactions (Issa *et al.*, 2023). These observed improvements are documented as statistically significant according to relevant tests; hence, blue-chip companies can count on blockchain integration to deliver an observable boost in the strength of authentication over the paradigm of traditional systems. This conclusion correlates with prior research that promotes blockchain as a potentially powerful means of strengthening the security of tokens through distributed trust systems (Nasrinasrabadi *et al.*, 2024).

The simulation also investigated scale and latency with BMFA systems as they exist in realistic digital settings. Even though the systems based on blockchain have greater overhead adduced by the consensus mechanism and transaction recording, the authentication time does not exceed reasonable boundaries in cases where the optimised blockchain architecture and lightweight cryptographic schemes are utilised (Oktian & Lee, 2020). The small overhead of authentication time over TMFA is the cost of much higher security. Also, the scalability test proves that BMFA can effectively support a growing number of users, especially when the use of permissioned or hybrid blockchain models with effective consensus protocols, such as Practical Byzantine Fault Tolerance (PBFT), is applied (Sousa *et al.*, 2018). This finding contributes to the views of Wang *et al.* (2019), according to which the implementation of optimised blockchain frameworks will enable the issue of scalability to be resolved without seriously affecting system performance.

The findings, as a whole, support the fact that blockchain-based multifactor authentication is a significant advancement compared to the traditional practices. Through the following: Increased data privacy due to immutable and decentralised records, A statistically significant increase in token security (entropy and mutual information of token), scalable or latency-tolerant authentication procedures applicable in practice, and the BMFA framework offer a secure and future-facing approach to the increasing issues related to digital systems security. The research adds to the existing research on the use of blockchain in cybersecurity and confirms that it is technically and operationally possible to incorporate blockchain into authentication procedures to improve the overall process (Li *et al.*, 2020; Nasrinasrabadi *et al.*, 2024).

5. CONCLUSION

The research was able to design and prove a Blockchain-Based Multifactor Authentication (BMFA) framework that would help improve the privacy, security, and confidentiality of data used in digital systems. Using massive computational simulations and performance evaluations, the framework was significantly tolerant to attacks by an adversary, increased token security, expanded scalability, and reduced latency compared to traditional multifactor authentication (TMFA) systems. The use of blockchain within MFA systems also became one of the most efficient ways to decrease the likelihood of the successful compromise of a system. The distributed structure of blockchain, along with the immutability of ledgers and verification systems based on smart contracts, eradicated the existence of any single points of failure and, to a large extent, rendered vulnerability to attacks much more complicated. Simulations always revealed a significant reduction in the adversary success probability within the BMFA framework, which is in line with previous studies that support distributed, tamper-resistant structural security (Li *et al.*, 2020; Alzhrani *et al.*, 2022; Conti *et al.*, 2018). Further, the quantitative analysis of the authentication token security in terms of Shannon entropy and mutual information corroborated the notion that the BMFA framework helps to increase the uncertainty and randomness of authentication tokens. This greatly increases the difficulty with which attackers are able to reuse or predict tokens, and this is essential to resisting replay and brute-force ripostes (Shannon, 1948; Esposito *et al.*, 2021; Issa *et al.*, 2023). These findings also confirmed that integration with blockchain technology limits the dependencies of interpretation of authentication events information, thereby diminishing the predictability of tokens and the vulnerability of sessions.

Scalability of the framework and its latency were also considered keenly. Although the concepts related to blockchains are prone to an overhead, the research revealed that permission blockchain frameworks, smart contract improvements, and lightweight cryptographic functions are capable of producing consistent low authentication latency within the scope of realisable thresholds. The results align with the earlier studies that presented the argument that optimised blockchain designs will be able to accomplish both scalability and security without dramatically affecting the responsiveness of the systems (Rahman *et al.*, 2024; Oktian & Lee, 2020; Sousa *et al.*, 2018). Taken together, this research gives a solid, scalable, and future-proof solution in the form of the blockchain-based multifactor authentication framework that is able to systematically overcome all the drawbacks of traditional authentication systems and build a positive change that can carry the world forward. It improves data privacy, tightens the token security, and enables low-latency authentication that can bear real-life applications. The research offers valuable information to the existing literature on the application of blockchain in cybersecurity and provides an adequate platform that future studies can build on in terms of streamlining blockchain-based authentication protocols within modern digital environments.

REFERENCES

Alabdulatif, A., Khalil, I., Yi, X., Alazab, M., & Guizani, M. (2025). Blockchain-based privacy-preserving authentication and access control model for e-health users. *Information, 16*(3), 219.

Ali, A. S. M., Ali, S., Ziaullah, K., Joo, M. I., & Kim, H. C. (2025). *IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage*. IEEE Access.

Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things, 23*, 100844.

Alzhrani, F. E., Saeedi, K. A., & Zhao, L. (2022). A taxonomy for characterizing blockchain systems. *IEEE Access, 10*, 110568-110589.

Barcelo, A., Queralt, A., & Cortes, T. (2022). Revisiting active object stores: Bringing data locality to the limit with NVM. *Future Generation Computer Systems, 129*, 425-439.

Cheng, G., Chen, Y., Deng, S., Gao, H., & Yin, J. (2021). A blockchain-based mutual authentication scheme for collaborative edge computing. *IEEE Transactions on Computational Social Systems, 9*(1), 146-158.

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452.

Cunha, T. B. D., & Manjappa, K. (2024). Private and consortium blockchain-based authentication protocol for IoT devices using PUF. *Journal of Communications and Networks, 26*(2), 166-181.

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management, 58*(2), 102468.

Gajmal, Y. M., & Udayakumar, R. (2021). Blockchain-based access control and data sharing mechanism in cloud decentralized storage system. *Journal of web engineering, 20*(5), 1359-1388.

Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023).

Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys, 55*(9), 1-43.

Khan, U. H., Khan, Q., Khan, L., Alam, W., Ali, N., Khan, I., ... & Khan, R. A. (2021). MPPT control paradigms for PMSG-WECS: A synergistic control strategy with gain-scheduled sliding mode observer. *IEEE Access, 9*, 139876-139887.

Lam, K. Y., Mitra, S., Gondesen, F., & Yi, X. (2021). ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities. *IEEE Internet of Things Journal, 9*(8), 5895-5908.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.*

Nasrinasrabadi, M., A Hejazi, M., Chaharmahali, E., & Hussein, M. (2024). *A Comprehensive Review of Blockchain Integration in Smart Grid with a Special Focus on Internet of Things.* Ehsan and Hussein, Mousa, A Comprehensive Review of Blockchain Integration in Smart Grid with a Special Focus on Internet of Things (August 10, 2024).

Nosenko, A., Cheng, Y., & Chen, H. (2023). Password and passphrase guessing with recurrent neural networks. *Information systems frontiers, 25*(2), 549-565.

Oduselu-Hassan, O. E. (2025). A Second-Order Imex-Rk Approach for Energy-Stable Phase Field Crystal Simulations. *Asian Basic and Applied Research Journal, 7*(1), 193-202.

Oduselu-Hassan, O. E., & Kenneth, O. (2024). Synergies between Machine Learning, Artificial Intelligence, and Game Theory for Complex Decision-Making. Artificial Intelligence, and Game Theory for Complex Decision-Making (November 15, 2024). *Asian Research Journal of Mathematics, 20*(11), 10-9734

Oktian, Y. E., & Lee, S. G. (2020). BorderChain: Blockchain-based access control framework for the Internet of Things endpoint. *IEEE Access, 9*, 3592-3615.

Oktian, Y. E., & Lee, S. G. (2020). BorderChain: Blockchain-based access control framework for the Internet of Things endpoint. *IEEE Access, 9*, 3592–3615.

Oladayo, O. H. (2025). Advancing Hybrid Numerical Methods for Nonlinear Stochastic Differential Equations: Applications in Complex Systems. *Asian Journal of Research in Computer Science, 18*(1), 124-132.

Rahman, A., Kundu, D., Debnath, T., Rahman, M., & Islam, M. J. (2024). *Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities.* arXiv preprint arXiv:2405.12550.

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal, 27*(3), 379–423.

Sharma, P., Jindal, R., & Borah, M. D. (2021). Blockchain-based decentralized architecture for cloud storage system. *Journal of Information Security and Applications, 62*, 102970.

Sousa, J., Bessani, A., & Vukolic, M. (2018). A Byzantine fault-tolerant ordering service for the Hyperledger Fabric blockchain platform. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 51–58.

Tran, L., Nguyen, T., Seo, C., Kim, H., & Choi, D. (2022). *A Survey on Password Guessing.* arXiv preprint arXiv:2212.08796.

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategies in blockchain. *IEEE Access, 7*, 22328–22370.

Zhai, P., He, J., & Zhu, N. (2022). Blockchain-based Internet of Things access control technology in intelligent manufacturing. *Applied Sciences, 12*(7), 3692.