https://dx.doi.org/10.4314/dujopas.v12i2a.14
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol.12 No. 2a June 2026*

Pilot Investigation on Security Enhancement for a Door Access Management for a Commercial Manufacturing Environment

Arnold Adimabua Ojugo[1], Margaret Dumebi Okpor[2], Kingsley Theophilus Igulu[3], Emeke Ugboh[4], Onome Taibat Asunogie[5], Rosemary Usiobaifo[6], Paul Avwerosuo Onoma[1], Tabitha Chukwudi Aghaunor[7], Amaka Patience Binitie[4], Peace Oguguo Ezzeh[4], Eferhire Valentine Ugbotu[8], and Samuel Ufuoma Okperigho[1]

[1]College of Computing,
Federal University of Petroleum Resources,
Effurun, Delta 330102,
Nigeria.

[2]Faculty of Computing,
Southern Delta University,
Ozoro, Delta 334111,
Nigeria.

[3]Faculty of Computing,
Ignatius Ajuru University of Education,
Port-Harcourt, Rivers 334111,
Nigeria.

[4]School of Science Education,
Federal College of Education (Technical),
Asaba, Delta 320212,
Nigeria.

[5]Faculty of Computing,
Edo University, Uzuaire,
Edo State 320212,
Nigeria.

[6]Faculty of Computing,
University of Benin,
Benin City, Edo State 340212,
Nigeria;

[7]School of Data Intelligence and Technology,
Robert Morris University,
Pittsburgh, PA15108,
United States of America;

[8]Faculty of Science,
Engineering and Environment,
University of Salford,
Manchester M54WT,
United Kingdom;

Email: ojugo.arnold@fupre.edu.ng;

**Author for Correspondence*

Abstract

The rapid rise in adoption for embedded systems to ease automatic systems deployment to advance data process platforms across businesses has continued to spurn various security challenges. Transition from key to a fusion with embedded units will continue to raise concerns. The proliferation of automated door access control lends itself to a centralized, wireless sensor network that is poised as a target of varying threats. Thus, it explores user factor authentication with demerits that include data corruption, credentials thefts, mishandling, misinformation, coordinated and subterfuge threats cum attacks, etc, compromising its reliance on a single point of access via the single point failure technique. This study uses a quasi-experimental framework to unveil challenges for door access management. Its security is enhanced via the blockchain-multifactor authentication scheme. Data was collected from five (5) experts at varying manufacturing industries in Nigeria with the ploy to help safeguard business resources. These, were chosen using the stratified sampling approach to explore and assess the proposed pilot scheme. The instrument was validated with a 0.05 level of significance. The blockchain-MFA scheme is a frontier domain to secure the management of physical access point from unauthorized users. Its decentralized structure with immutable records access helps to address key limitations in conventional access security such as single-point failures and records vulnerabilities. The fusion of MFA (PIN + RFID + Biometrics) with blockchain approach has advanced the field of IoT-security, provisioning a system that both improves access control, and ensures forensic traceability of all authentication attempt; Making it a viable solution for institutions with high-security needs. Our result shows that the pilot system security can be enhanced for improved security, transparency, and auditability that dissuades single-point failures, threats, and credential/records vulnerabilities.

Keywords: Blockchain, identity access management; multifactor authentication, Door Access,

INTRODUCTION

Increased demand for convenient, safe, and secure access to residential cum commercial infrastructure has continued to drive the consequent adoption and integration of cyber-connected systems with the adaptation of embedded systems in the form of Internet of Things (IoT) (Tahir et al., 2025). And in turn, necessitates a more robust, security-conscious environment as more user devices become networked. Users today have moved from the key-based to radio-frequency identification (RFID) door access systems (Eboka et al., 2025). However, the rising trends in adversarial attacks have rendered such systems increasingly vulnerable, ushering threats such as key duplication, theft, loss, and spoofing (Obruche et al., 2024). This adoption has changed the security landscape for door access management. This utilization of IoTs is necessitated by its open-source nature, via-a-vis their ease of adaptability, portability, and user-friendliness, which has continued to advance them as an ideal/better choice for promoting cyber-physical, intelligent systems. Their integration with ESP microcontrollers is found to be effective in managing data encryption functions in data exchange cum transmission (Stolojescu-Crisan et al., 2021). Furthermore, the inherent versatility therein of IoTs, alongside its capability to grant developers cum researcher an improved platform for robust designs that enable deployment of a cost-effective, secure, and scalable approach for next-generation, cyber-enhanced security solutions (Kakarlapudi & Mahmoud, 2021; Onoma, Ako, et al., 2025).

The adoption of IoTs by businesses today helps to further advance user inclusivity on tailored solutions and platforms; And in turn, ease the solution's reachability cum availability as targeted goods and services for consumers (Okofu et al., 2024). Thus, the rapid proliferation of threats has led businesses to increase their adoption of authentication modes/schemes that are today poised to help identify/verify a user device. For real-time monitoring of exchange amongst interacting devices, enhancing management capabilities, and enabling encrypted exchanges that mitigate attack risks (Yoro et al., 2025), businesses must be equipped with platforms and solutions that validate exchanges through user authentication. This feat is also advanced by the post-COVID era, which has witnessed a rapid rise in remote data processing. Remote management capability grants businesses the ability to securely oversee IoT utilization for every scenario (Aghaunor et al., 2025). Advances to secure data transfer have birthed authentication via the utilization of factoids across platforms with a variety of settings. To address organizational needs for security and data integrity, users must urgently confront several critical issues with sensitive data access with schemes that: (a) ensure interoperability across platforms explored for exchange, (b) maintain data confidentiality and privacy, and (c) secure user devices, systems, and other accompanying resources. To prevent unauthorized access to sensitive resources, device manufacturers typically implement methods and programs that authenticate designated users prior to enabling the requisite access permission and rights to these devices (Binitie et al., 2025, 2026).

Authentication thus seeks to effectively identify a user over a platform – validating their identity via submitted user data. While the submitted user data (factoid or factor) confirms the authenticity of a user as either genuine/authorized or malicious/unauthorized, these factoids are traditionally grouped into knowledge, ownership, and biometric factors (Binitie et al., 2025). Rapid advances in technology today have ushered in a variety of means to verify a user's identity, and the primary goal of user authentication is to protect data, sensitive network applications, and resources from unauthorized (compromised device) access as well as against varied forms of coordinated online/offline exploits (Aghware et al., 2024; Kanagamalliga et al., 2025). Through community-driven security practices, IoT-systems adapt these new frontiers as tools and techniques to efficiently tackle emerging threats/exploits as well as safeguard against user device compromises cum unauthorized access. In commercial door access systems, the management of sensitive (user) credentials is crucial and critical. The unauthorized access of such resources can significantly degrade administration and system performance. Thus, heightened security is quite imperative for effective task coordination, control of sensitive records (Akazue et al., 2023, 2024), safeguard of user credentials against data corruption via tampering (Oladele et al., 2024; Omede et al., 2024), theft, or mishandling, and the efficient exchange of records among authorized personnel.

To address the inherent challenges, this study advances questions that will propagate the need (where necessary) for user authentication via a multifactor strategy, vis-à-vis enhancing the security of the system using blockchain technology for the manufacturing industry. The main contributions are summarized as follows: (a) a secure, remote processing environment via the consequent adoption of IoT using its do-it-yourself (DIY) approach, (b) increased support for operational productivity that dissuades unauthorized user access to data and other resources, and (c) a comprehensive performance and security assessment demonstrating the capability of the existing door access system to enhance data (user credentials) confidentiality, access integrity, and regulatory compliance readiness.

Multifactor Authentication Approach: A Review

User access to door management and control using the key-based approach cum scheme allows for a physical (on-site, in-person) authentication. It is often required that the user comply with a variety of protocols involving the use of the physical key to unlock the door therein. The correctness of the challenge-and-response protocol validates a user, and access rights cum permission are granted (Arachchige et al., 2024). However, the problem with loss of key, placement forgetfulness, and damage of physical key – consequently, led to the adoption of IoT-based door access management and control that explores the option of wireless sensor networks (WSN). This mode often explores an approach for which a user is verified and validated through a series of challenge-and-response feedback between the interacting user device and the system (Ratazzi et al., 2014). However, an adversary can readily impersonate a legitimate user by presenting the correct credentials. This necessitated the exploration of authentication schemes – as a central nexus to enhance network security, data privacy, and confidentiality; While provisioning credential audit trails, user access traceability, improved manageability, and authorization control for data resources (Ejeh et al., 2026).

Authentication over remote processing cum management can explore a variety of forms, namely single-factor, two-factor, and multifactor approaches (Aparecido Cardoso et al., 2019). It is noteworthy that the Single-Factor Authentication (SFA) prioritized simplicity and user-friendliness via its reliance on a single-factor/level authentication. Many of such systems are vulnerable to guessing attacks, shoulder surfing, dictionary attacks, and rainbow-table attacks (Nur et al., 2025), etc. In addition, the non-adherence with the minimum requirements in complexity for the creation/utilization of the factoids as well as the frequent exchange of factoids, was found to further compromise user accounts and degrade overall system performance. Recognizing these shortcomings ushered in the Two-Factor Authentication (2FA). It combines a layer of factoid over another, creating two levels as added security to effectively authenticate a user. Inherent inadequacies of this approach – birthed the multifactor scheme; Which often fuses the three (3) factors of knowledge, ownership, and biometrics to result in a credential/profile that helps establish a legitimate connection between a legitimate user and a resource pool (Alamleh et al., 2023). The knowledge factor represents something the user knows, such as a password or a personal identification number, etc. The ownership factor represents something the user has, such as a smartcard, tokens, etc; while the biometrics factor represents something that the user is, such as biometric gaits, and/or behavioral patterns (Geteloma et al., 2025).

Many platforms today utilize multifactor authentication (MFA) schemes, especially with their fusion of biometrics, due to their stronger resistance against various forms of exploits. The adopting system often allows user enrolment of factors via scanning of user gaits onto a template to enable its consequent matching (Aparecido Cardoso et al., 2019). The user's gait is scanned and stored to create a template used for rapid retrieval. The systems then match the scanned data against the stored templates, ensuring that only authorized users gain access to the door system. This efficient process improves verification as well as mitigates vulnerabilities associated with lost access methods (Jairam et al., 2022). Despite the plethora of benefits proffered by factor authentication, challenges persist that can be addressed through emerging technologies, such as blockchain. Businesses today still utilize embedded units to manage resources across such door access distributed systems. Their reliance on centralized resources to ease access, it creates a security risk and potential breaches. While authentication does enhance security, blockchain adds an extra protection layer for data resources (Aghaunor et al., 2026).

The Blockchain Solution

Distributed systems, by design, are poised to collect, process, and store records that IoT units may access (Nartey et al., 2021). These rely on connected resources to ease access, which in turn creates security risks cum potential attacks. The inherent features of the blockchain model include immutability, which prevents the unauthorized alteration cum tamper of records. Adoption of the blockchain scheme improves user trust, enhances security, and facilitates the exchange of sensitive resources as it offers transparency, improved authentication, consensus records verification, and unique data-sharing capabilities (Sheng et al., 2023). Blockchain has proven effective in addressing numerous access management challenges while providing opportunities that help with its effective fusion of emerging techs (Malik et al., 2024). To facilitate the successful deployment of blockchain applications, we must address issues of interoperability and standardization (Northrop, 2025). The blockchain yields a tamper-proof, distributed database that is maintained and validated across a network of connected nodes. Thus, it efficiently addresses the inherent challenges in conventional databases via timestamped nodes to prevent tampering and corruption (Allam et al., 2024). The blockchain is explored in various forms: (a) permissioned, (b) permissionless, (c) consortium, and (d) hybrid. Each blockchain form has its specific application domain, its corresponding benefits, and set of drawbacks that can either advance or restrict its usage (Brizimor et al., 2024; Malasowe et al., 2024; Obasuyi et al., 2024; Olaniyi et al., 2023).

Its inherent features, such as immutability, prevent unauthorized alteration of records and data. Adopting blockchain technology can improve user trust, enhance security, and facilitate the exchange of sensitive records (Deon & Best, 2025). Blockchain apps today offer transparency, improved authentication, consensus verification, and unique record-sharing capabilities. Blockchain has proven effective in addressing numerous information management challenges while providing opportunities to integrate with emerging technologies. To facilitate the successful development of blockchain applications, it is imperative that we also address the issues of interoperability and standardization. Blockchain mechanisms have recently been explored to support cross-provider trust negotiation and auditability. However, such platforms continue to face scalability and latency challenges in highly dynamic cloud environments, alongside persistent concerns regarding policy enforcement consistency and trust orchestration (Salam et al., 2024).

Study Gaps and Motivation

Various frameworks have been proposed to enhance data privacy and resource security in blockchain-based MFA solutions; however, many of these applications have also been found to have shortcomings when deployed, especially in door access management infrastructures with multiple vendors (Wu et al., 2024). Rehman et al. (Rehman, 2024) investigated decentralized authentication for the federated blockchain. It showed greater scalability demands and eliminated centralized trust in door access control. Rivera et al. (Jose Diaz Rivera et al., 2024) explored blockchain encryption to strengthen data confidentiality. While it improved security, it also substantially incurred greater computational overhead, higher operational costs, and user throughput latency, as factors that impeded its practical implementation cum deployment. Omosor et al. (Omosor et al., 2025) examined anonymization over a blockchain-MFA door access, which reported stronger resistance to re-identification attacks; however, the scheme birthed notable trade-offs that rely on tedious-to-audit security solutions that seek to reinforce the need for a more unified, interoperable system (Aleisa et al., 2025).

Thus, this study is motivated by the following crucial research questions, namely:

1. There is still a lack of an end-to-end security architecture that simultaneously and coherently addresses privacy preservation, trust management, and access control across the door access management and control infrastructure. Existing solutions focused on isolated components, which raises interoperability concerns and exposes cross-domain data exchanges to additional risks (Cena, 2024).
2. Second, cryptographic techniques continue to suffer from a persistent trade-off between efficiency and security. While some approaches provide enhanced confidentiality, they also birth significant execution overhead and operational costs that impede realtime applicability (Brijwani et al., 2024). Achieving the balance in enhanced security, improved usability, and computational efficiency remains a challenge.
3. Third, the trust feature for the door access control and management mechanisms remains insufficient. Trust for such a scenario must be continuously monitored and updated to reflect compliance status, service reliability, and systemic behavioral risk. The existing system relies on centralized trust, which degrades scalability, with increased throughput delay and infrastructure latency with practical deployment (Addae et al., 2024; Bamashmos et al., 2024).
4. Fourth, existing solutions are largely vendor-centric and insufficiently interoperable across the heterogeneous IoT (Almadani et al., 2023). And exposes the ecosystem to greater vulnerability and risk of emerging threats such as weaker authentication, data/resources theft, corruption and tampering, ineffective data encryption, etc (Sinha, 2024).

These collectively motivate the need for an adaptive and interoperable security framework tailored specifically for modern door access management and control systems, leveraging the IoT ecosystems.

MATERIALS AND METHODS

The study employs a quasi-experimental design that fuses the qualitative and quantitative schemes. The qualitative approach focuses on the deployment of a questionnaire derived via literature synthesis and expert consultation, whilst the quantitative scheme involves assessment of research questions of selected MFA, blockchain, and emerging trends across the IoT ecosystem in lieu of the door access management and control environment. Feedback was retrieved from both experts and participants using the current system via a questionnaire for the construction of the proposed system as in Figure 1.

The system implements a blockchain-based multifactor authentication strategy for the door access management and control system (Anthony-Akhutie et al., 2025). Thus, by definition and implementation, its security orchestration enforces the blockchain access policies with support for user/device verification via its business logic and smart contracts (Osilonya et al., 2026). To mitigate insider threats, external breaches, and unauthorized access attempts – the existing system advances a tightly coupled framework (see Figure 1) that enables a fine-grained, real-time authentication and adaptive authorization on the blockchain-based door access management and control system: (a) Door Access Control, (b) Authentication Model with Identity Access Management (OAuth 2.0), and (c) Blockchain Architecture (Geteloma et al., 2024; Okeke & Omojola, 2025).

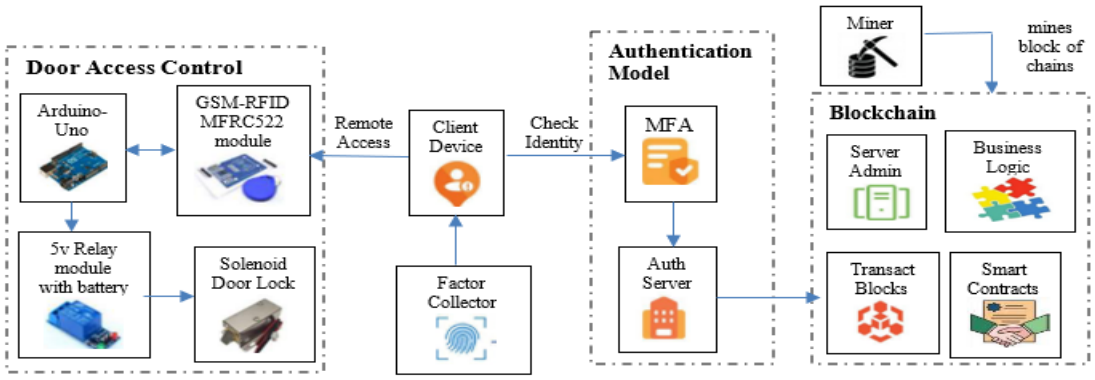

Figure 1. Blockchain-based MFA Workflow for Door Access Management and Control

Users are validated on the blockchain via its trust management policies that explore a hybrid cryptographic scheme using AES-256 for bulk encryption and RSA-2048/ECC for asymmetric key exchange. Furthermore, its distributed trust is propagated via an Ethereum Blockchain to enhance auditability and accountability via its smart contracts. Authentication events, access requests, and computation activities are immutably recorded to strengthen traceability and non-repudiation (Halder et al., 2024; Ugbotu, Ako, et al., 2025). Together, these components provide continuous verification and dynamic policy enforcement across distributed cloud environments.

RESULTS AND DISCUSSION

Results

Table 1 yields the resulting questionnaire used to gather information from the experts, is analyzed thus:

Table 1. Expert's Response from Questionnaire for the Blockchain-MFA solution

Q	Framework	Expert's Response				
		1	**2**	**3**	**4**	**5**
1	Does your organization utilize the most current and cutting-edge Multifactor Authentication Architecture?	Yes	No	No	Yes	No
2	Are regulatory compliance requirements (like HIPAA, GDPR, ISO/SAE 21434, or IEC 62443) a significant factor influencing your authentication architecture decisions?	Yes	Yes	No	Yes	Yes
3	Do you believe that seamless user experience (biometric authentication and single sign-on) significantly improve end-user adoption of MFA systems?	Yes	Yes	Yes	Yes	Yes
4	Do you have challenges with MFA implementation due to BYOD policies, legacy system compatibility, or network connectivity limitations in manufacturing environments?	Yes	Yes	No	Yes	No
5	Would security measures like honeypots, behavioural analysis, and threat intelligence integration significantly enhance your organization's authentication security posture?	Yes	Yes	Yes	No	Yes
6	Do you use progressive onboarding (gradually introducing authentication factors over time) and risk-based adaptive authentication to minimize user resistance to the adoption of MFA-based solutions?	No	Yes	No	No	Yes
7	Is clear communication (explaining why additional verification is required), real-time feedback, and accessibility support essential for designing a user-friendly MFA interface?	Yes	Yes	Yes	Yes	Yes
8	Are phishing attacks, session hijack, credential stuffing, and insider threats among the most significant security risks your organization faces with the current MFA implementations?	Yes	Yes	Yes	Yes	Yes
9	Does your organization wish to explore alternatives such as Zero-Trust, enhanced homographic schemes, differential encryption, LRaft, etc	Yes	Yes	Yes	Yes	Yes

The following explanations were reached owing from the Questionnaire:

1. **Q1, Q2, and Q4** seeks to establish the current state of MFA implementations, regulatory constraints, and technical challenges – as baseline against which the proposed blockchain-based adaptive MFA solution is positioned. The 80% agreement on hybrid MFA usage and implementation challenges validates the need for an enhanced, decentralized approach.
2. **Q3, Q6, and Q7** seek to assess the factors that influence user adoption of the automated door access management and control. The unanimous agreement (100%) on Q3 and Q7 confirms that seamless user experience and clear UI/UX design are critical for adoption. The lower agreement on Q6 (40%) reveals that progressive onboarding is underutilized, representing an opportunity for the proposed solution to differentiate itself through adaptive, user-friendly authentication workflows.
3. **Q4** directly addresses implementation requirements by identifying real-world challenges (BYOD policies, legacy compatibility, network limitations) that the solution must overcome. The 80% agreement confirms these are widespread concerns requiring architectural solutions such as offline authentication support, API integration layers, and flexible deployment models.
4. **Q5 and Q8** seeks to identify the attack/threat landscape (phishing, session hijacking, credential stuffing, insider threats) and security enhancement opportunities (honeypots, behavioural analysis, threat intelligence). The 100% agreement on Q8 confirms that the zero-trust architecture and continuous validation mechanisms are essential security requirements. The 80% agreement on Q5 demonstrates expert recognition that advanced security measures are necessary.
5. **Q9** directly addresses the various implementation concerns as in the study vis-a-vis identifies real-world challenges (DIY policies, interoperability, legacy compatibility, network limitations) that the solution must overcome. The 90% agreement confirms it as widespread concerns requiring architectural solutions such as offline authentication support, flexible deployment models, and API integration layers. The experts noted that the implementation of a zero-trust model/policy on the resultant blockchain-based MFA solution for the door access management and control will address inherent challenges herein experienced.

DISCUSSION

Key Findings from Expert Responses

1. **Strong Consensus on Critical Factors (100% Agreement):** ll five experts unanimously agreed that seamless user experience significantly improves adoption (Q3), proper UI/UX design principles are essential (Q7), and phishing/session hijacking/credential stuffing represent significant threats (Q8). This unanimous consensus validates the study's focus on adaptive MFA with user-friendly interfaces and comprehensive security measures addressing identified threat vectors. This agrees with Onoma et al. (2025) that the credential spoofing for data access can easily be detected via the utilization of enhanced voice dynamic warping scheme to track dynamic voice decibels (Onoma, Agboi, et al., 2025) as well as help to effectively track socially-engineered threats and coordinated subterfuge attacks as agreed by (Agboi et al., 2025; Ugbotu, Emordi, et al., 2025).
2. **High Agreement on Implementation Context (80%):** Four out of five experts confirmed that their organizations use hybrid MFA (Q1), face regulatory compliance pressures (Q2), encounter implementation challenges with BYOD/legacy systems (Q4), and would benefit from advanced security measures (Q5). This strong majority validates the practical relevance of the proposed solution's features: permissioned blockchain for compliance, API

integration for legacy systems, and zero-trust architecture with advanced threat detection. The utilization of cross-border regulations even with the implementation of HIPAA and GDPR as agreed by Oladele et al. (2024) and Omede et al. (2024) was leveraged as provisioning the legal framework and backdrop for permissioned blockchain compliance (Oladele et al., 2024; Omede et al., 2024).

3. **Gap Identification - Progressive Onboarding (40% Current Usage):** Only two experts reported using progressive onboarding and risk-based adaptive authentication (Q6), despite unanimous agreement that seamless UX improves adoption (Q3). This gap reveals an opportunity: organizations recognize the importance of user experience but have not yet implemented adaptive authentication mechanisms. The proposed blockchain-based adaptive MFA system directly addresses this gap by dynamically adjusting authentication requirements based on risk context, device trust level, and user behaviour patterns. Thus, the need for the fusion of the zero-trust approach over the blockchain model with multi-cum-hybrid cloud-integration for improved device level trust with policies that help users adjust to next-level authentication and transaction validation as agreed by Aghaunor et al. (2026).

CONCLUSIONS

This study advances several notable theoretical and technical contributions as thus: (a) a unified blockchain-MFA solution that enhances security with zero-trust model, (b) advances an AI-driven threat detection, enabling improved anomaly detection and reducing insider-threat response latency, (c) an enhanced privacy-preserving computation pipeline for secure multi-party computation and homomorphic encryption achieving data-resources utility retention; and (d) a blockchain-enabled identity management mechanism that leverages smart contracts to support authentication and demonstrates the practical viability of decentralized identity within adaptive federated environments. In terms of cryptographic performance, the proposed homomorphic encryption pipeline demonstrates an average operation time of approximately 450ms per operation under the evaluated configuration. This performance is supported by: (a) differential privacy configured at $\varepsilon = 0.1$ with 99.2% utility retention, and (b) a 34% processing speed improvement compared with conventional differential privacy implementations.

The study demonstrated significant improvements in security, and auditability compared to traditional centralized access control mechanisms. The implementation of blockchain-based multifactor authentication represents a breakthrough in securing physical access points, particularly in environments where data protection and unauthorized access pose critical risks. The decentralized structure and immutable records provided by blockchain address key limitations in conventional access systems, including single-point failures and credential vulnerabilities. This research has successfully demonstrated a working prototype of a 3-factor authentication system – integrating the knowledge (PIN), possession (RFID), and inherence (biometrics) as secured by the blockchain architecture with zero-trust-fused IoT ecosystem. The system not only improves access control but also ensures forensic traceability of every authentication attempt, making it a viable solution for institutions with high-security needs.

REFERENCES

Addae, S., Kim, J., Smith, A., Rajana, P., & Kang, M. (2024). Smart Solutions for Detecting, Predicting, Monitoring, and Managing Dementia in the Elderly: A Survey. In *IEEE Access* (Vol. 12). IEEE. https://doi.org/10.1109/ACCESS.2024.3421966

Agboi, J., Emordi, F. U., Odiakaose, C. C., Idama, R. O., Jumbo, E. F., Oweimieotu, A. E., Ezzeh,

P. O., Eboka, A. O., Odoh, A., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Aghaunor, T. C., Binitie, A. P., Onochie, C. C., Nwozor, B., & Ejeh, P. O. (2025). Phishing Website Detection via a Transfer Learning based XGBoost Meta-learner with SMOTE-Tomek. *Journal of Fuzzy Systems and Control*, *3*(3), 181–189. https://doi.org/10.59247/jfsc.v3i3.325

Aghaunor, T. C., Agboi, J., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Odiakaose, C. C., Eboka, A. O., Ezzeh, P. O., Geteloma, V. O., Binitie, A. P., Orobor, A. I., Nwozor, B., Ejeh, P. O., & Onochie, C. C. (2025). EcoSMEAL: Energy Consumption with Optimization Strategy via a Secured Smart Monitor- Alert Ensemble. *Journal of Fuzzy Systems and Control*, *3*(3), 190–196. https://doi.org/10.59247/jfsc.v3i3.319

Aghaunor, T. C., Ugbotu, E. V., Ugboh, E., Onoma, P. A., Emordi, F. U., Ojugo, A. A., Geteloma, V. O., Idama, R. O., & Ezzeh, P. O. (2026). Investigating Security Enhancement in Hybrid Clouds via a Blockchain-Fused Privacy Preservation Strategy: Pilot Study. *Journal of Computing Theories and Applications*, *3*(4), 428–442. https://doi.org/10.62411/jcta.15508

Aghware, F. O., Okpor, M. D., Adigwe, W., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Ejeh, P. O., Taylor, O. E., Ako, R. E., & Geteloma, V. O. (2024). BloFoPASS: A blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria. *International Journal of Informatics and Communication Technology*, *13*(2), 178–187. https://doi.org/10.11591/ijict.v13i2.pp178-187

Akazue, M. I., Edje, A. E., Okpor, M. D., Adigwe, W., Ejeh, P. O., Odiakaose, C. C., Ojugo, A. A., Edim, E. B., Ako, R. E., & Geteloma, V. O. (2024). FiMoDeAL: pilot study on shortest path heuristics in wireless sensor network for fire detection and alert ensemble. *Bulletin of Electrical Engineering and Informatics*, *13*(5), 3534–3543. https://doi.org/10.11591/eei.v13i5.8084

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using blockchain network: a case of Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1623–1633. https://doi.org/10.11591/ijeecs.v29.i3.pp1623-1633

Alamleh, H., AlQahtani, A. A. S., & Smadi, B. Al. (2023). *Secure Mobile Payment Architecture Enabling Multi-factor Authentication*. https://doi.org/10.48550/arXiv.

Aleisa, M. A., Science, C., Computer, C., & Sciences, I. (2025). Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2025.3529309

Allam, A. H., Gomaa, I., Zayed, H. H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: a survey. *Cluster Computing*, *0123456789*. https://doi.org/10.1007/s10586-024-04357-y

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. https://doi.org/10.1016/j.iot.2023.100844

Anthony-Akhutie, P., Omosor, J. C., Onoma, P. A., Ojugo, A. A., Ako, R. E., Agboi, J., Odiakaose, C. C., Max-Egba, A. T., Geteloma, V. O., Niemogha, S. U., & Abdullahi, M. B. (2025). SEMAEco-IoT: A Secured IoT-based Smart Energy Monitor and Alert for Enhanced Energy Conservation and Optimization. *FUPRE Journal of PetroScience*, *1*(1), 150–166.

Aparecido Cardoso, J. A., Ishizu, F. T., De Lima, J. T., & Pinto, J. D. S. (2019). Blockchain Based MFA Solution: the use of hydro raindrop MFA for information security on WordPress websites. *Brazilian Journal of Operations & Production Management*, *16*(2), 281–293. https://doi.org/10.14488/BJOPM.2019.v16.n2.a9

Arachchige, K. G., Branch, P., & But, J. (2024). An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks. *Sensors*, *24*(10), 3083. https://doi.org/10.3390/s24103083

Bamashmos, S., Chilamkurti, N., & Shahraki, A. S. (2024). Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. *Sensors*, *24*(11). https://doi.org/10.3390/s24113575

Binitie, A. P., Okofu, S. N., Okpor, M. D., Anazia, K. E., Ojugo, A. A., Egbokhare, F. A., Egwali, A., Ezzeh, P. O., Ako, R. E., Geteloma, V. O., Aghaunor, T. C., Ugbotu, E. V., & Onyemenem, S. I. (2025). MoBiSafe: an obfuscated single factor authentication mode to enhance secured USSD channel transaction in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *40*(1), 426. https://doi.org/10.11591/ijeecs.v40.i1.pp426-436

Binitie, A. P., Onyemenem, S. I., Anujeonye, N. C., Ojugo, A. A., Egbokhare, F. A., & Aghaunor, T. C. (2026). A Graph-Augmented Isolation Forest Using Node2Vec and GraphSAGE for Mobile User Behavior Anomaly Detection. *Journal of Computing Theories and Applications*, *3*(3), 369–383. https://doi.org/10.62411/jcta.15494

Brijwani, G. N., Ajmire, P. E., Jewani, V., Thawani, P. V., Mohammad, D., Junaid, M. A., Khan, T., & Pawar, D. S. (2024). HealthShield: A Blockchain-Based Electronic Health Recording System with Enhanced Security Algorithm for Immutable and Confidential Health Data Management. *International Journal of Scientific Research in Science and Technology*, *11*(3), 794–814. https://doi.org/10.32628/ijsrst24113234

Brizimor, S. E., Okpor, M. D., Yoro, R. E., Emordi, F. U., Ifioko, A. M., Odiakaose, C. C., Ojugo, A. A., Ejeh, P. O., Abere, R. A., Ako, R. E., & Geteloma, V. O. (2024). WiSeCart: Sensor-based Smart-Cart with Self-Payment Mode to Improve Shopping Experience and Inventory Management. *Social Informatics, Business, Politics, Law, Environmental Sciences and Technology Journal*, *10*(1), 53–74. https://doi.org/10.22624/aims/sij/v10n1p7

Cena, J. (2024). Multi-Factor Authentication Paradigms for Securing Industrial Internet of Multi-Factor Authentication Paradigms for Securing Industrial Internet of Things (IIoT) Assets. *Bulletin of Electrical Engineering and Informatics*, *21*(May), 23–46.

Deon, L., & Best, T. (2025). Zero Trust Security and Cloud Security : A Modern Approach to Cyberattack Prevention Date : February , 2025. *ResearchGate*, *1*(February). https://doi.org/10.13140/RG.2.2.24739.57126

Eboka, A. O., Aghware, F. O., Okpor, M. D., Odiakaose, C. C., Okpako, A. E., Ojugo, A. A., Ako, R. E., Binitie, A. P., Onyemenem, S. I., Ejeh, P. O., & Geteloma, V. O. (2025). Pilot study on deploying a wireless sensor-based virtual-key access and lock system for home and industrial frontiers. *International Journal of Informatics and Communication Technology*, *14*(1), 287–297. https://doi.org/10.11591/ijict.v14i1.pp287-297

Ejeh, P. O., Osilonya, V. O., & Isizoh, A. (2026). Trust-constrained Intelligence for Realtime Clinical Reasoning in Centralized Healthcare Information Systems : A Pilot Study. *Computing, Information Systems, Development Informatics & Allied Research Journal*, *17*(1), 1–24. https://doi.org/10.22624/AIMS/CISDI/V17N1P1x

Geteloma, V. O., Aghware, F. O., Adigwe, W., Odiakaose, C. C., Ashioba, N. C., Okpor, M. D., Ojugo, A. A., Ejeh, P. O., Ako, R. E., & Ojei, E. O. (2024). AQuamoAS: unmasking a wireless sensor-based ensemble for air quality monitor and alert system. *Applied Engineering and Technology*, *3*(2), 70–85. https://doi.org/10.31763/aet.v3i2.1409

Geteloma, V. O., Okpor, M. D., Ugboh, E., Anazia, K. E., Odoh, A., Agboi, J., Abere, R. A., Aghaunor, T. C., Ugbotu, E. V., Odiakaose, C. C., & Ojugo, A. A. (2025). Investigating Risk Level in Maternal Mortality via a 3ConFA Feature Fused SMOTE-Tomek Balancing with Attention-Guided BiGRU Scheme : A Pilot Study. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *11*(3), 59–80. https://doi.org/10.22624/AIMS/BHI/V11N3P5x

Halder, R., Das Roy, D., & Shin, D. (2024). A Blockchain-Based Decentralized Public Key Infrastructure Using the Web of Trust. *Journal of Cybersecurity and Privacy*, *4*(2), 196–222. https://doi.org/10.3390/jcp4020010

Jairam, A., Halevi, T., & Raphan, T. (2022). Improving Mobile Device Security by Embodying and Co-adapting a Behavioral Biometric Interface. *Frontiers in Computer Science*, *4*. https://doi.org/10.3389/fcomp.2022.754716

Jose Diaz Rivera, J., Muhammad, A., & Song, W.-C. (2024). Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. *IEEE Open Journal of the Communications Society*, *5*, 2792–2814. https://doi.org/10.1109/OJCOMS.2024.3391728

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). Design and Development of a Blockchain-Based System for Private Data Management. *Electronics*, *10*(24), 3131. https://doi.org/10.3390/electronics10243131

Kanagamalliga, S., Rajalingam, S., Kannan, A., & Karthikeyan, M. (2025). Biometric and IoT Integration for Secure and Remote Door Access Control Using Fingerprint Recognition and GSM Technology. *E3S Web of Conferences*, *619*, 03013. https://doi.org/10.1051/e3sconf/202561903013

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *NIPES - Journal of Science and Technology Research*, *6*(2), 293–311. https://doi.org/10.5281/zenodo.12617068

Malik, P., Pandey, A., Swarnkar, R., Bavarva, A., & Marmat, R. (2024). *Blockchain-Enabled Edge*

Computing for IoT Networks Blockchain-Enabled Edge Computing for IoT Networks. *March*. https://doi.org/10.55041/IJSREM28718

Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., & Diawuo, K. (2021). On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives. *Wireless Communications and Mobile Computing*, *2021*, 1–25. https://doi.org/10.1155/2021/6672482

Northrop, J. (2025). *Interoperability Challenges And Solutions In Multi-Vendor Iot Ecosystems For Agriculture*. *July*.

Nur, M. J., Setiadi, D. R. I. M., Ojugo, A. A., & Nguyen, M. T. (2025). Improving Customer Churn Prediction Using Domain-Driven Feature Engineering, Resampling, and CatBoost with Explainability Extensions. *2025 International Seminar on Application for Technology of Information and Communication (ISemantic)*, 493–499. https://doi.org/10.1109/ISemantic67418.2025.11291801

Obasuyi, D. A., Yoro, R. E., Okpor, M. D., Ifioko, A. M., Brizimor, S. E., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ako, R. E., Geteloma, V. O., Abere, R. A., Atuduhor, R. R., & Akiakeme, E. (2024). NiCuSBlockIoT: Sensor-based Cargo Assets Management and Traceability Blockchain Support for Nigerian Custom Services. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *15*(2), 45–64. https://doi.org/10.22624/aims/cisdi/v15n2p4

Obruche, C. O., Abere, R. A., & Ako, R. E. (2024). Deployment of a virtual key-card smart-lock system: the quest for improved security, eased user mobility and privacy. *FUPRE Journal of Scientific and Industrial Research*, *8*(1), 80–94.

Okeke, K., & Omojola, S. (2025). Enhancing Cybersecurity Measures in Critical Infrastructure: Challenges and Innovations for Resilience. *Journal of Scientific Research and Reports*, *31*(2), 474–484. https://doi.org/10.9734/jsrr/2025/v31i22868

Okofu, S. N., Anazia, K. E., Akazue, M. I., Okpor, M. D., Oweimieotu, A. E., Asuai, C. E., Nwokolo, G. A., Ojugo, A. A., & Ojei, E. O. (2024). Pilot Study on Consumer Preference, Intentions and Trust on Purchasing-Pattern for Online Virtual Shops. *International Journal of Advanced Computer Science and Applications*, *15*(7), 804–811. https://doi.org/10.14569/IJACSA.2024.0150780

Oladele, J. K., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Abere, R. A., Nwozor, B., Ejeh, P. O., & Geteloma, V. O. (2024). BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange. *Journal of Computing Theories and Applications*, *1*(3), 231–242. https://doi.org/10.62411/jcta.9509

Olaniyi, O. O., Okunleye, O. J., Olabanji, S. O., Asonze, C. U., & Ajayi, S. A. (2023). IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience. *Asian Journal of Research in Computer Science*, *16*(4), 354–371. https://doi.org/10.9734/ajrcos/2023/v16i4397

Omede, E. U., Edje, A. E., Akazue, M. I., Utomwen, H., & Ojugo, A. A. (2024). IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System. *Journal of Computing Theories and Applications*, *1*(3), 273–283.

https://doi.org/10.62411/jcta.9541

Omosor, J. C., Onoma, P. A., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Akhutie-Anthony, P., & Okperigho, S. U. (2025). Security Enhancement using Multifactor Authentication Strategy for the Solenoid Door Access Control and Management: A Pilot Study. *FUPRE Journal of Scientific and Industrial Research*, *6*(3), 80–94.

Onoma, P. A., Agboi, J., Ugbotu, E. V., Aghaunor, T. C., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Binitie, A. P., Ezzeh, P. O., Ejeh, P. O., Onochie, C. C., Geteloma, V. O., Emordi, F. U., Orobor, A. I., & Obruche. (2025). Attrition Rate Prediction using a Frequency-Recency- Monetization-based SMOTEEN-Boosted Approach. *MSIS - International Journal of Advanced Computing and Intelligent System*, *3*(1), 1–11.

Onoma, P. A., Ako, R. E., Anazia, K. E., Oghorodi, D., Okpako, A. E., Onochie, C. C., Geteloma, V. O., Ezzeh, P. O., Ugboh, E., Ojugo, A. A., Eboka, A. O., & Idama, R. O. (2025). Quest for Ground-Truth or Stochastic Myth by Leveraging the AI-Powered Wearable Device for Dementia Disease Detection: A Pilot Study. *FUPRE Journal of Scientific and Industrial Research*, *9*(3), 343–358.

Osilonya, O. V., Ejeh, P. O., & Isizoh, A. (2026). Enhanced Centralized Medical Records Security In a Zero-Trust-based MFA Framework Using Formal Verification of Role-Based Access Control. *Journal of Advances in Mathematical and Computational Sciences*, *14*(1), 31–56. https://doi.org/10.22624/AIMS/MATHS/V14N1P3

Ratazzi, P., Aafer, Y., Ahlawat, A., Hao, H., Wang, Y., & Du, W. (2014). A Systematic Security Evaluation of Android ' s Multi-User Framework. *MoST*, *December 2020*.

Rehman, N. (2024). *Strengthening Financial Institutions ' Data Security with Blockchain Technology and Zero Trust Security : A Comprehensive Cyber Defense Strategy Date : November , 2024*. *November*. https://doi.org/10.13140/RG.2.2.21956.85127

Salam, A., Abrar, M., Amin, F., Ullah, F., Khan, I. A., Alkhamees, B. F., & Alsalman, H. (2024). Securing Smart Manufacturing by Integrating Anomaly Detection with Zero-Knowledge Proofs. *IEEE Access*, *12*, 36346–36360. https://doi.org/10.1109/ACCESS.2024.3373697

Sheng, W. J., Kasmin, I. F., Amin, S., & Zainal, N. K. (2023). Addressing user perception and implementing Hedera Hashgraph and voice recognition into Multi-Factor Authentication (MFA) system. *International Journal of Data Science and Advanced Analytics*, *4*, 194–201. https://doi.org/10.69511/ijdsaa.v4i0.165

Sinha, S. (2024). Blockchain for Enhancing IoT Privacy and Security. *International Journal of Innovative Research in Computer Science and Technology*, *12*(2), 106–110. https://doi.org/10.55524/ijircst.2024.12.2.18

Stolojescu-Crisan, C., Crisan, C., & Butunoi, B.-P. (2021). An IoT-Based Smart Home Automation System. *Sensors*, *21*(11), 3784. https://doi.org/10.3390/s21113784

Tahir, H. T., Aghaunor, T. C., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Abere, R. A., Agboi, J., & Aherobo, V. O. (2025). Enhancing Security with Blockchain-Enabled Privacy Preservation for Multi-and-Hybrid Cloud Environment: A Pilot Study. *Advances in Multidisciplinary & Scientific Research Journal Publication*, *16*(4), 25–44.

https://doi.org/10.22624/AIMS/CISDI/V16N4P3

Ugbotu, E. V., Ako, R. E., Odoh, A., Oghorodi, D., Okpako, A. E., Aghaunor, T. C., Emordi, F. U., Ugboh, E., Agboi, J., Odiakaose, C. C., Ojugo, A. A., Geteloma, V. O., Abere, R. A., Idama, R. O., Eboka, A. O., Ezzeh, P. O., Onochie, C. C., Oweimieotu, A. E., Ojo, B., & Onoma, P. A. (2025). Equipping the GREDDIoMT Device with Early Behavioural Risk Detection of Dementia via a Pre-Activated SENet fused BiGRU. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *11*(3), 36–56. https://doi.org/10.22624/AIMS/BHI/V11N3P4

Ugbotu, E. V., Emordi, F. U., Ugboh, E., Anazia, K. E., Odiakaose, C. C., Onoma, P. A., Idama, R. O., Ojugo, A. A., Geteloma, V. O., Oweimieotu, A. E., Aghaunor, T. C., Binitie, A. P., Odoh, A., Onochie, C. C., Ezzeh, P. O., Eboka, A. O., Agboi, J., & Ejeh, P. O. (2025). Investigating a SMOTE-Tomek Boosted Stacked Learning Scheme for Phishing Website Detection: A Pilot Study. *Journal of Computing Theories and Applications*, *3*(2), 145–159. https://doi.org/10.62411/jcta.14472

Wu, J., Xue, N., Li, Z., Hong, X., Zhao, Y., Huang, X., & Zhang, J. (2024). SPCL: A Smart Access Control System That Supports Blockchain. *Applied Sciences*, *14*(7), 2978. https://doi.org/10.3390/app14072978

Yoro, R. E., Okpor, M. D., Akazue, M. I., Okpako, A. E., Eboka, A. O., Ejeh, P. O., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Ako, R. E., Geteloma, V. O., Onoma, P. A., Max-Egba, A. T., Ibor, A. E., Onyemenem, S. I., & Ukwandu, E. (2025). Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner. *Plos One*, *20*(6 June), 1–20. https://doi.org/10.1371/journal.pone.0326571