International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 15, No. 4, December 2026, pp. 1532~1545
ISSN: 2252-8776, DOI: 10.11591/ijict.v15i4.pp1532-1545

Deploying enhanced security for blockchain MFA wireless virtual-key access management for industrial frontiers

Andrew Okonji Eboka[1], Fidelis Obukohwo Aghware[2], Margaret Dumebi Okpor[3], Bridget Ogheneovo Malasowe[2], Ejaita Abugor Okpako[2], Arnold Adim Ojugo[4], Reuben Akporube Abere[4], Amaka Patience Binitie[1], Rita Erhovwo Ako[4], Innocent Sunny Onyemenem[1], Adesuwa Inaya[1], Victor Ochuko Geteloma[4]
[1]Department of Computer Science, School of Secondary Education (Science), Federal College of Education (Technical), Asaba, Nigeria
[2]Department of Computer Science, University of Delta, Agbor, Nigeria
[3]Department of Cybersecurity, Faculty of Info Technology, Delta State University of Science and Technology, Ozoro, Nigeria
[4]Department of Computer Science, College of Computing, Federal University of Petroleum Resources, Effurun, Nigeria

Article Info

Article history:

Received Aug 3, 2024
Revised Jun 23, 2026
Accepted Jul 5, 2026

Keywords:

Blockchain-MFA
Door access management
Home security
Virtual key lock
Wireless sensor network

ABSTRACT

The increased adoption of automated devices and its utilization to advance data processing in many facets of societal tasks and demand operations has continued to birth accompanying security challenges. Physical infrastructures today integrates within them automated units to upscale traditional issues. The recent proliferation of automated door access with innovative embedded units employs a centralized design with single-factor authentication, which has proven inefficient for safeguarding restricted environments. Other challenges of data corruption, theft, mishandle of user credentials, all of which can be compromised due to its single point of access control. This study advances enhanced access security for virtual key door infrastructure via a blockchain-MFA strategy. It implements secure, scalable access control with a 3-layered framework of PIN + RFID + Biometric, validated using smart contracts on a blockchain network. The results demonstrated improvements in security, transparency, and auditability compared to traditional door access control, especially against adversarial attacks from single-point failures and credential vulnerabilities. Our prototype unit demonstrates 3-factor authentication for improved security that ensures forensic traceability of every authentication attempt, making it a viable solution for institutions with high-security needs.

*This is an open access article under the **CC BY-SA** license.*

Corresponding Author:

Andrew Okonji Eboka
Department of Computer Science, School of Science Education
Federal College of Education (Technical)
Asaba, Delta State, Nigeria
Email: eboka.andrew@fcetasaba.edu.ng, ebokaandrew@gmail.com

1. INTRODUCTION

There is today an increased demand vis-à-vis the requisite importance of user convenience, safety and secure access to both residential and commercial infrastructure [1]. Evidence abounds that it has continued to necessitate a security-conscious environment, with traditional security to building infrastructure utilizing either the conventional key mode [2], or the recent adoption of radio frequency identifier (RFID) door access [3]. Whichever the scenario, major challenges inherent in this traditional design is their ease of compromise and susceptibility to key duplication, theft, loss, and other forms cum mode of spoofing [4] which exposes the traditional door access system to a plethora of security risks. However, the emergence and

integration of the internet of things (IoTs) that allow the use of sensors, microcontrollers, and other ancillary components to aid full automation has ushered in a paradigm shift vis-à-vis the continued ease to door access infrastructure and operations [5]. The fusion with microcontrollers has continued to gain widespread proliferation due to its increased popularity, open-source nature [6], eased mobility [7], portability in allied components [8], ease, versatility [9], and cross-platform deployment with interoperability [10]. These features have continued to position them as a realistic, custom-fit solution [11] for a variety of domain tasks, that also includes door (access) control frameworks.

These IoT solutions have, at their nexus, the Arduino unit [12] equipped with the ESP controllers [13] for its processing unit, which is responsible for retrieval and management of data as well as effectively coordinating the system's overall processing cum operation. The choice of Arduino is attributed to its flexibility to seamlessly integrate various sensor units [14], its robustness and reuse in related tasks [15], and its black-box adaptability [16] to suitably achieve sophisticated control(s). In addition, the Arduino leans on its capability to offer low-cost, do-it-yourself (DIY) [17], and custom-effective solution(s) for researchers aiming at security enhancements with varying configurations and design settings for IoT applications. Emphasis on the DIY paradigm [18], [19] allows researchers to model, hands-on build, modify, and implement lightweight model-targeted solutions fit to meet specific needs; while its open-source nature advances agile [20] collaboration with cross-cutting innovations that enable the continued enhancement cum deployment of new features. The lightweight framework utilizes software algorithms that play crucial roles in performance optimization and accuracy, especially with embedded systems security architecture via multifactor biometric-based authentication [21], [22], among other integrations with the door access control systems. The adoption of IoT systems with biometric algorithms has contributed to black-box adaptation, robustness, added reliability [23], and flexibility in modern biometric recognition systems [24] as utilized in door access management and control systems.

While IoT continues to birth new solutions, we acknowledge their inherent susceptibility and proneness to attacks/breaches, forcing many systems to adopt the fusion of biometric modalities (i.e. fingerprint, facial, iris, and thermal) as key functionalities to foster secure data exchange with real-time monitoring over such platforms. These are exercised over mobile smartphones via the integration of the SIM900 as a means to extend/expand the capabilities of the access management control system. Its remote interaction between a user and the system facilitates real-time monitoring and control management for the Arduino-based, IoT-enabled solution. While this extension allows authorized users to remotely (un)lock a door via apps on their smartphones, it also adds an extra layer for eased user acceptability [25], improved satisfaction cum convenience [26], user satisfaction, and the required system's flexibility. The SIM900 advances support for encrypted data transfer between legitimate users and the system, to dissuade potential attacks [27] and protect the device from unsuspecting compromises [28], [29]. While targeting operational effectiveness by extending its capability in cases for which direct physical access control is limited [30], [31].

Remote capabilities for door access control management are quite valuable today, especially with the rise in the proliferation of smartphones that enable users to manage secure access to restricted areas in and out of both residential and commercial buildings at varying locations [32]. Many such systems have explored and adopted fingerprint biometric recognition, which in many climates has been found to be efficient, safe, and secure [33], [34]. This is because, at its enrollment stage, all participating users' fingerprints are scanned, and their templates are thereafter stored in the record base to ease retrieval checks via a challenge-response that matches the template scan with stored user gaits [35]. It utilizes the template for future scans to validate user identity as well as ensure that only authorized users are granted access to the infrastructure. The optimized challenge-response match process advances quick and accurate template matching that helps to minimize throughput time to validate a user identity [36]. The adoption of biometrics has continued to efficiently ease the dynamics of theft, loss, and forgetfulness associated with a user's physical key(card), as well as eliminating the obvious need to memorize passwords/PINs. In addition, this scheme also addresses the growing questions and concerns for more security-conscious access control with its key merit that allows for ease in customization within a user community. To foster community-driven solutions where security not only evolves rapidly in response to emergent techs, but also faces adversaries seeking to gain unauthorized access while evading detection, compromising a network infrastructure to user device information.

Thus, our study seeks to contribute as follows:

a) Implement an IoT-based door access control mechanism for solenoid doors as installed in buildings.
b) Deploy remote capability that helps identify users via a multifactor authentication (MFA) scheme, ported on the mobile-based application framework that synchronizes/match user profile data with the Auth-template
c) Enhance the framework's security using blockchain technology to ensure immutability of transactions
d) Comparing the performance of this approach to existing methods.

Section 2 describes authentication schemes and blockchain approaches to IoT-based door access control via the literature reviewed, materials and methods explored, and the evaluation metric utilized in the study, and Section 3 concludes the main findings and provides further development directions for further studies.

2. LITERATURE REVIEW

2.1. Review of related literature

The potential applications of an Arduino-based IoT system with MFA as implemented on a mobile smartphone are quite vast. It ranges from securing personal resources/properties to managing door access and real-time control for large infrastructure [37]. With increased demand for more secure, flexible, scalable, and adaptable door access control systems, our study seeks to proffer valuable insights via technical requirements, methods and materials, design configurations, user-defined settings and considerations as well as experimental results to assert the efficacy of this scheme. Thus, we advance support studies as a backdrop cum foundation for further experimentation and enhancement that helps with a sustainable evolution in IoTs for door access control. Its ease of accessibility and portability assure its ability to deploy across various contexts (commercial and residential) to proffer a versatile solution fit for different needs. Thus, the fusion with an Arduino unit, GSM module, and biometric recognition tech [38], has since been acknowledged as a promising solution to modern door access management and real-time control challenges.

Extensive studies have been conducted on the subject of this fusion with fingerprint (biometric) as widely adopted due to its uniqueness and security benefits [39]. Its reliability has been demonstrated via its high accuracy with a low false acceptance rate (FAR). With a variety of models deployed to enhance the precision and efficiency in fingerprint matching (i.e. minutiae and pattern)-some works have integrated fingerprint with other biometric modalities such as facial recognition [40] as a mode to further enhance its security in access control and management systems. Its effectiveness for large-scale identification has eased its adoption, which can also be attributed to its scalability and applicability [10]. Such advances have continued to showcase the critical role of biometrics towards improved acceptance in modern access management and control systems. In addition, other customizable solutions have explored the integration of RFID as a mode to enable users to gain door access via RFID cards, while allowing for realtime monitor cum alert via mobile apps [41].

While some researchers have proffered home automation systems controlled via Bluetooth for improved ease of usage and convenience - its fusion to harness the capabilities of the Arduino-based solution with various sensors and modules has continued to emphasize its ability to deploy sophisticated access control mechanisms. This eased versatility with the Arduino-based IoT solutions is integrated across the GSM platform to ease remote management, monitor/alert as well as upscale the embedded functionality for door access management and control systems [42]. This design approach uses the GSM unit to facilitate a range of remote actions via SMS, which yields an extra layer of security. While this improves access inclusivity, its effectiveness of remote capabilities of access control systems. The convenience, efficiency, and capability to operate a secure door access management and control system remotely have become increasingly imperative for today's mobile-connected and digital society [43], where users are often required to remotely manage and control their access from different locations [44]. Thus, our study aims to demonstrate the effectiveness of a door access management and control system enhanced using a blockchain-based MFA strategy (with fingerprint and facial recognition) from mobile smartphone apps as modes to enhance system security, while offering ease of use, convenience, and flexibility via this DIY [45], open-source nature in IoTs, offering a practical-fit solution that also encourages innovation and scenario-targeted customization.

2.2. Explored methodology

Building an artifact must be poised to address some unresolved challenges, for which its evaluation must unveil the performance therein, resolving the purported challenges as in Figure 1. Thus, we explore a framework that combines both behavioral and design paradigms, which: (a) offers a process to understand, execute, and evaluate the model, and (b) contributes to our adopted/adapted design via the identified business needs. Studies have claimed that the goal of behavioral-science research is to find the truth - wherein, whereas the inherent goal for design-science research is to build and evaluate a proposed utility product that will advance frontiers of science and technology. Additionally, they noted that truth and utility are very much inseparable. Thus, the proposed artifact to be produced and implemented in relation to design-science research are more often than not a fully finished information system product. Thus, studies have posited that an artifact represents an innovation that defines the ideas, technical capabilities, practices, and products with the help of which the design, analysis, implementation, and usage of data systems can be accomplished [46].

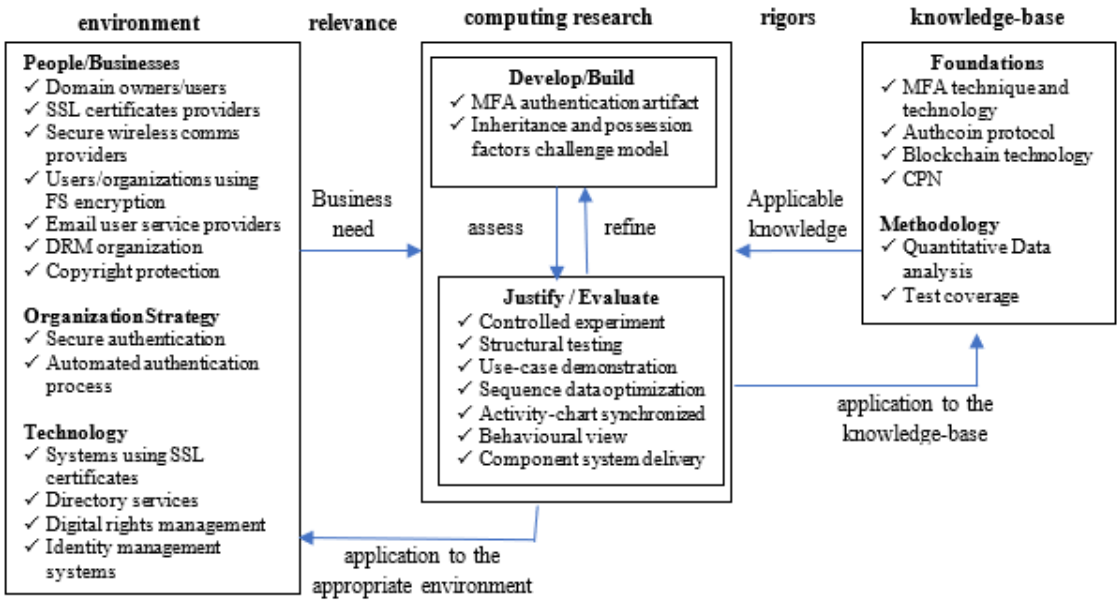


Figure 1. Proposed design framework

2.3. Experimental design framework

Our proposed (enhanced) door access management and control system explores a structured but sequential data flow as in Figure 2, which integrates multiple authentication layers with blockchain-based validation to ensure high-level security, transparency, and auditability. Each stage of the process builds upon the previous one, and authentication is only successful when all stages are correctly completed and verified on the blockchain. The flow ensures both system integrity and user accountability via its immutability and smart contract automation to validate and log each event. The detailed operational sequence is as in Figure 2.

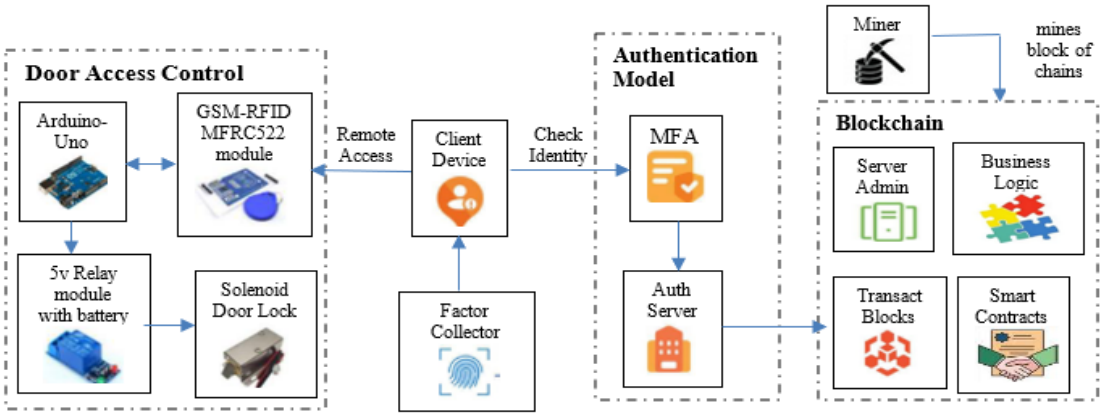


Figure 2. Schematic diagram of the proposed blockchain-MFA fused IoT solution

Its detailed operational sequence is outlined as follows,

a) Step 1 - Factor collection - Here, the system initializes the authentication process immediately when a legitimate user swipes their RFID-card via the card reader as installed on the artifact. The RFID reader is connected to the ESP32 microcontroller as ported on the Arduino board. The system then extracts each user's unique identifier (UID) from the card and explores a challenge-response scheme to ascertain/verify its authenticity via the MFA server (auth_server), as in Figure 2. Where the RFID UID is valid and accepted as responded to by the MFA (auth_server), it is encrypted as a token in its server's registry and passed on to the blockchain network, so that the system proceeds to the next stage; Else, access is immediately denied, and a failed attempt alert is logged on the audit server of the blockchain [47].

b) Step 2 - PIN verification with hash-match: Where the RFID verification is successful, the system explores a challenge-response mechanism that prompts the user to input their PIN using the attached keypad module. The inputted PIN is hashed and transmitted securely as a token to the auth_server and blockchain for comparison against the template (user) stored hashed PIN. Where the hash matches the stored value, this confirms the identity based on the knowledge factor. If it fails, access is denied and the attempt alert is logged on the audit server [48].
c) Step 3 - Token generated for mobile app authentication: upon successful PIN verification, the system generates a one-time password/token (OTP/OTT) that serves as the session's hook, or reference identifier (RID). This token is not revealed to the blockchain directly, but is logged internally with the auth_server alone and associated with a verified user. Its function is to serve as a bridge to initiate the mobile app for the authentication process – so that once validated, the user can perform remote management access and control of the door. The token ensures that only users who passed the RFID-and-PIN challenge-response proceed to application-level verification [49], [50].
d) Step 4 – Mobile app input for blockchain token verification: Each user is then required to open the accompanying mobile app to input the OTP/OTT as generated in the previous stage. The token is then hashed and forwarded via the app to the blockchain, which then executes the smart contract to validate the token against the stored template as generated and associated with each user's session. If the token is correct, the user is allowed to proceed with biometric (fingerprint) ownership verification and user identity validation. This stage validates the authenticity of the user interacting with the door access and control system with real-time connectivity over the IoT-based solution [51], [52].
e) Step 5 – Biometric user identity validation: the system prompts for biometric authentication, which can be performed via the mobile app. This design configuration adds an extra layer of synchronization and security that dissuades spoofing attacks from adversaries. The fingerprint minutiae data as captured is then compared to the registered fingerprint template, stored securely in its encrypted form on both the auth_server and blockchain. Where the fingerprint matches, this confirms the inherence factor [53], [54].
f) Step 6 – Access and physical door (un)lock: Upon successful completion of all previous authentication steps with tokens as verified and validated between the auth_server and blockchain – a final confirmation of access granted is sent through the smart contract to the ESP32 microcontroller, which then activates the solenoid (door) lock to physically unlock the door. This mechanical action affirms a successful multi-factor authentication as well as marks the end of the session [55], [56].
g) Step 7 – Blockchain logs with audit trail: Where the biometric token is unsuccessful, an audit trail is logged onto the blockchain. In addition, at every stage therein, the smart contract logs every authentication event on the blockchain with time-stamped entries. Whether an access attempt is successful or fails at any stage (RFID, PIN, token, or biometric), all events are transparently and immutably recorded. This ensures an audit trail that administrators or auditors can review at any time without the risk of tampering or deletion [57], [58].

This stepwise flow ensures that no single authentication factor can compromise access security. The use of blockchain helps with user login credential validation and event logging, which brings an additional layer of decentralization [59], transparency, and resilience. Thus, addressing the critical weaknesses inherent in conventional door access management and control systems [60]. The entire system is designed to be modular, scalable, and suitable for deployment in high-security environments, with the algorithm listed in Algorithm 1.

Algorithm 1. Listing of the Blockchain-based MFA strategy

```
Input: user_input (PIN, RFID, biometric_signature), blockchain_credentials,
mobile_confirmation
Output: access_granted, access_denied
Initialize system components && connect to blockchain //Initializing the blockchain
and auth_server for candidate nodes
// Step 1: PIN Verification
prompt user to enter PIN : hash entered PIN
if hashed_PIN matches blockchain.stored_PIN then generate session_token
    store session_token on blockchain : log as success
else: log "PIN verification failed" on blockchain.stored_PIN: display "Access
Denied" && exit
endif

// Step 2: RFID Validation
prompt user_scan RFID
if RFID_matches user_token on blockchain.stored_token then update session_token on
blockchain
    log as success
else: log "RFID validation failed" on blockchain.stored: display "Access Denied" &&
```

```
exit
endif
// Step 3: Biometric Confirmation via Mobile App
send session_token to user.mobile_device
listen.wait for biometric.confirm
if biometric.confirm_received && signature == verified then grant.access
   activate solenoid.door_mechanism : log "Access Granted" on blockchain.store
else: log "Biometric verification failed" on blockchain.stored
    display "Access Denied"
endif
   reset authentication flags
end
```

The proposed system tackles the limitations of traditional access control by introducing a blockchain-based MFA approach/framework that integrates PIN, RFID tags, and biometric fingerprint recognition. Its key improvements used to address previous bottlenecks include [61]: (a) it utilizes decentralized blockchain to resolve the backdrop of a central database authentication with records stored on a distributed ledger technology that ensures fault tolerance and eliminates single point of failure [62], (b) it utilizes the distributed modular framework implemented with smart contracts and the distributed identity management to validate new access points (users) prior onboarding without reconfiguring the entire system [63], [64], (c) it exercises a triple-layered MFA scheme (i.e. biometric, PIN, and RFID) to ensures access is granted only to verified/validated users, and remains secure even with 1-or-2 factors compromised, (d) it explores the blockchain's business logic and smart contracts to provision audit trails with logs such that all access events (and failed attempts) are recorded immutably to aid forensic review, and improved user-trust level [65], and (e) it resolves traditional system's poor flexibility via business logic that handles access permissions, provide updates, and access control logic as dynamically programmable and automatically enforceable [66].

2.4. Technical system requirement and design configuration

Our proposed system was designed with the following parameters: The physical components as assembled include: (a) The ESP32-WROOM microcontroller module was programmed via the Arduino IDE with ESP32 board support package. It had built-in Wi-Fi capabilities, configured to establish secure connections to the blockchain. Its deep-sleep mode was implemented to optimize power consumption during idle periods. Interrupt-based wake-up mechanisms were configured for the keypad and RFID reader. (b) The Auth_Server interfaced a 4×4 matrix keypad with the ESP32 via GPIO pins (13-12-14-27-26-25-33-32). The MFRC522 RFID reader integrates a GSM module connected via the SPI protocol for MOSI-23, MISO-19, SCK-18, and SS-5. In addition, we interfaced the 16×2 LCD with the I2C communication protocol (SDA-21, SCL-22). The solenoid lock is controlled by a 5V relay, connected to GPIO-15 and a 9 V battery, and (c) Power management uses 5v/2A DC adapter on a backup 3.7 V 2000 mAh LiPo battery with a TP4056 controller (and an automatic power source switching circuit for uninterrupted operation and a monitor that alerts battery status).

Components were mounted on a weatherproof (IP65)- rated enclosure with a custom PCB fabricated to minimize wiring complexity. Tamper detection switches were installed to detect unauthorized access attempts to the enclosure, while the artefact, as in Figure 3, was installed on a standard door frame with concealed wiring. Table 1 shows the hardware configuration. Figure 3 shows the initial state of the artifact, and Figure 4 shows an activated RFID card on the proposed system. The software requirements for deploying and operating the system yield the configuration as in Table 2.



Figure 3. Door access control artifact



Figure 4. RFID-card authentication activated

Table 1. Hardware requirements

Component	Specification	Function	Quantity
Microcontroller	ESP32-WROOM-32	Core processing unit	1
RFID Reader	MFRC522	RFID card authentication	1
Matrix Keypad	4×4 Membrane	PIN code input	1
LCD Display	16×2 I2C	User feedback interface	1
Relay Module	5V Single Channel	Control electromagnetic lock	1
Electromagnetic Lock	12V 600lbs Holding Force	Secure door locking mechanism	1
Power Supply	5V/2A DC Adapter	Primary power source	1
Backup Battery	3.7V 2000mAh LiPo	Power redundancy	1
Charge Controller	TP4056	Battery management	1
Voltage Regulator	LM2596	Power stabilization	1
PCB	Custom Designed	Component integration	1
Enclosure	IP65 Weatherproof	Environmental protection	1
RFID Cards	ISO/IEC 14443A	User credentials	2

Table 2. Software requirements

Software	Version	Purpose
Arduino IDE	1.8.19	ESP32 programming environment
ESP32 Board Package	2.0.5	Hardware support for ESP32
Remix IDE	Web-based	smart contract development and testing
Flutter SDK	3.10.0	Mobile application development
Dart	3.0.0	Programming language for Flutter
Solidity	0.8.0	Smart contract programming language
Web3.js	1.8.2	JavaScript library for blockchain interaction
Truffle Suite	5.7.0	Blockchain development framework
Ganache	7.5.0	Local blockchain for testing
Android Studio	2023.1.1	Android application development and testing
Xcode	14.3	OS application development and testing
Visual Studio Code	1.77.0	Code editor with extensions
Git	2.40.0	Version control system
Postman	10.13.0	API testing tool
Firebase Console	Web-based	push notification services

3. FINDINGS AND RESULT DISCUSSION

3.1. Authentication performance

This metric evaluates the overall system performance on its authentication accuracy, speed, and consistency in validating legitimate users while rejecting unauthorized attempts. A total of ten (10) trials were conducted to observe how each authentication layer (i.e. RFID, PIN, token-OTP, and biometric) contributes to performance and how quickly each cycle is completed using the success rate, false rejection rate (FRR), FAR, and average response time as in Table 3. In addition, Figure 5 shows OTP verification, while Figure 6 shows final user identity validation with blockchain login.

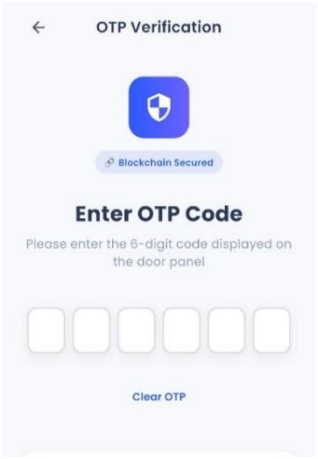


Figure 5. The OTP verification page

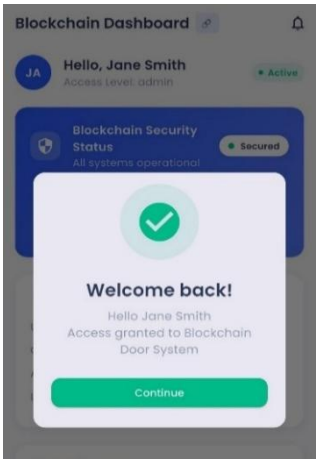


Figure 6. Final verification with blockchain login

Table 3. Performance evaluation with benchmark models

Trial No.	User Type	Input Factors	Auth Result	Time in Secs	Remarks
1	Legitimate User	Valid RFID, PIN, Token, Biometric	Success	3.2	All factors correct
2	Legitimate User	Valid RFID, wrong PIN	Failure	2.1	Blocked at PIN stage
3	Intruder	Cloned RFID	Failure	1.5	RFID not registered
4	Legitimate User	Valid RFID, PIN, expired token	Failure	2.9	Token expired
5	Legitimate User	All correct factors	Success	3.0	Smooth flow
6	Legitimate User	Biometric mismatch	Failure	3.1	Blocked at final stage
7	Legitimate User	All correct	Success	3.4	Slight biometric delay
8	Intruder	Token replay attempt	Failure	2.5	Rejected by smart contract

The authentication performance trials show that the system successfully validated all legitimate users with correct credentials while blocking unauthorized attempts at every stage. 3-out-of-8 trials were recorded as being successful; while, 5-trials were denied due to spoofing, incorrect inputs, or expired tokens. The average time for successful authentication login was approximately 3.2secs – demonstrating its realtime capability, and further confirms the FAR and FRR of 0% as properly configured sessions. This affirms the system's high authentication accuracy, its resistance to user misuse, and its operational efficiency, making it suitable for secure access deployment.

3.2. Blockchain performance

We assess the blockchain performance based on its efficiency, responsiveness, and reliability of the smart contract as it underpins access management and control process. Blockchain operations include template match, and credentials verification. These evaluate its impact on the overall system speed, transaction success, data immutability, and integrity assurance. Thus, we assess the transaction confirmation time, smart contract response time, and logging integrity were analyzed across multiple trials as in Table 4.

Table 4. Performance evaluation with benchmark models

Trial No.	Auth Triggered	Smart Contract Action	Blockchain Time (s)	Log Entry Created	Result
1	RFID Match	Token granted	1.4	Yes	Success
2	PIN Hash Verification	Token generated	1.6	Yes	Success
3	Token Input via App	Token validated	1.3	Yes	Success
4	Expired Token Attempt	Smart contract rejected token	1.2	Yes (logged as denied)	Rejected
5	Replay Attack Attempt	Smart contract flagged duplicate token	1.1	Yes	Rejected
6	Biometric Success	Final approval logged	1.5	Yes	Success
7	Tampered Request	Smart contract ignored invalid input	1.2	Yes	Rejected
8	Auth Triggered	Smart Contract Action	Blockchain Time (s)	Log Entry Created	Result

The trials confirm that the blockchain layer consistently responded within 1.1seconds to 1.6 seconds, demonstrating fast and stable smart contract execution for identity verification and logging. All authentication actions-including approvals, rejections, and invalid attempts – were accurately logged on the

blockchain, confirming the immutability and integrity of the event history. Importantly, the smart contract successfully prevented replay and tampering attempts, reinforcing its role as a trustless decision-maker in the system. Overall, the blockchain component proved to be efficient, secure, and transparent, with negligible latency impact. It enabled a decentralized verification framework that is auditable and resistant to manipulation, positioning the system well for use in high-security environments.

3.3. System reliability

To assess the flexibility, robustness, adaptability cum consistency of the developed blockchain-based MFA system, a series of reliability tests were conducted. These tests measured the system's behavior under repeated, valid access attempts, varied time intervals, and different user inputs. The aim was to determine how reliably the system performs authentication without failure, lag, or inconsistency across multiple sessions. Table 5 summarizes the outcomes of repeated successful authentication attempts performed over several trials. It shows how consistently the registered users were authenticated across multiple sessions without failure. Its average response time ranged between 3.00-to-3.70-secs – indicating minimal latency and delay were experienced even under varying conditions that include: (a) delayed token input and (b) reduced fingerprint scanner visibility [67].

Table 5. Performance evaluation with benchmark models

Trials	User Type	Authentication Attempted	Time (s)	Result	Remarks
1	Registered User	RFID → PIN → Token → Biometric	3.1	Success	Smooth and consistent
2	Registered User	RFID → PIN → Token → Biometric	3.3	Success	No delay observed
3	Registered User	RFID → PIN → Token (delayed) → Biometric	3.5	Success	Token expiration handled
4	Registered User	RFID → PIN → Token → Biometric	3.0	Success	Fast response
5	Registered User	RFID → PIN → Token → Biometric	3.2	Success	Consistent performance
6	Registered User	RFID → PIN → Token → Biometric (low light)	3.7	Success	Slight biometric delay

In addition, each trial successfully completed an authentication cycle even with faults (single point of failure) and/or rejecting valid inputs, which confirms the system's high reliability, stability, and real-time responsiveness. These, further validate the proposed system's effectiveness as practically deployed in a secure access environment where uptime and dependability are critical. The system demonstrated exceptional reliability during its 30-day test period with a resultant uptime of 0.997. It showed no errors or latency for remote SMS commands, which highlighted its effectiveness on remote management capabilities. Furthermore, our backup outperformed the proposed design specification, providing 1098 seconds of operational time efficiency (as compared to the targeted 720 seconds). This extended operation time enhances its suitability for critical security applications as well as demonstrates its ability to recover from network cum other various faults. A 1.000 recovery rate, with an average recovery time of 4.2 seconds, demonstrates the effectiveness of the proposed system's offline fallback mechanisms implemented in the ESP32 firmware. This resilience ensures that the authentication system remains functional even in environments with unstable network connectivity.

4. CONCLUSION

The proposed system integrates three authentication layers of PIN, RFID, and biometric verification as managed via the blockchain's smart contracts. Its mobile application and IoT-based access mechanism were also developed to demonstrate the functionality of the model in a real-time setting. Key components include: (a) the ESP32 interfaced with RFID readers, biometric sensors, and an LCD, (b) a blockchain with smart contracts deployed on the Ethereum testnet for credential validation, to ensure immutable log records, and decentralized access control, and (c) a mobile app ported on a smartphone for biometric (fingerprint) recognition, verification, and access management. The system was evaluated for authentication accuracy, latency, resistance to spoofing and tampering attacks, and overall operational efficiency.

The results demonstrated significant improvements in security, transparency, and auditability compared to traditional centralized access control mechanisms. The implementation of blockchain-based MFA 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. The study demonstrates a working prototype of a 3-factor authentication integrating knowledge (PIN), possession (RFID), and inherence (biometrics)-secured by blockchain and IoT technologies. The system improves access control and ensures forensic traceability of every authentication attempt, making it a viable solution for institutions with high-security needs.

ACKNOWLEDGMENTS

We wish to acknowledge the support from Federal College of Education (Technical), Asaba, Nigeria, the Federal University of Petroleum Resources Effurun, Nigeria, and the University of Delta Agbor, Nigeria, for the utilization of the requisite laboratories. We also thank our colleagues in no small measure.

FUNDING INFORMATION

The authors state that no funding was involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Andrew Okonji Eboka	✓		✓	✓		✓		✓	✓	✓		✓	✓	✓
Fidelis Obukohwo Aghware		✓		✓	✓		✓		✓	✓	✓			✓
Margaret Dumebi Okpor	✓		✓		✓			✓	✓	✓			✓	✓
Bridget Ogheneovo Malasowe		✓		✓		✓	✓		✓	✓	✓			✓
Ejaita Abugor Okpako	✓			✓		✓		✓	✓	✓		✓	✓	✓
Arnold Adim Ojugo	✓	✓	✓		✓	✓		✓	✓	✓		✓	✓	
Reuben Akporube Abere	✓		✓	✓		✓	✓		✓	✓	✓			✓
Amaka Patience Binitie		✓	✓			✓	✓		✓	✓	✓			✓
Rita Erhovwo Ako	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓
Innocent Onyemenem		✓	✓		✓		✓		✓	✓	✓		✓	✓
Adesuwa Inaya	✓		✓		✓			✓	✓	✓		✓	✓	✓
Victor Ochuko Geteloma		✓	✓		✓	✓	✓		✓	✓	✓	✓		✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

Data availability does not apply to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] J. Wu *et al.*, "SPCL: a smart access control system that supports blockchain," *Applied Sciences (Switzerland)*, vol. 14, no. 7, 2024, doi: 10.3390/app14072978.
[2] W. L. Hsu, J. Y. Jhuang, C. S. Huang, C. K. Liang, and Y. C. Shiau, "Application of internet of things in a kitchen fire prevention system," *Applied Sciences (Switzerland)*, vol. 9, no. 17, 2019, doi: 10.3390/app9173520.
[3] A. A. Aribisala, A. M. Adebimpe, and O. O. Fagbohun, "Development of an automatic door access control system using fingerprint and passcode verification technology," *Arid Zo. J. Eng. Technol. Environ.*, vol. 21, no. 4, pp. 1054–1062, Dec. 2025, doi: 10.63958/AZOJETE/2025/21/04/014.
[4] A. S. Khan *et al.*, "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network," *IEEE Access*, vol. 11, pp. 20524–20541, 2023, doi: 10.1109/ACCESS.2023.3249969.
[5] P. Ratazzi, Y. Aafer, A. Ahlawat, H. Hao, Y. Wang, and W. Du, "A systematic security evaluation of android's multi-user framework," in *MoST*, 2014, no. December 2020, pp. 23–35.

[6] H. Jo and Y. I. Yoon, "Intelligent smart home energy efficiency model using artificial TensorFlow engine," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, 2018, doi: 10.1186/s13673-018-0132-y.

[7] A. O. Eboka and A. A. Ojugo, "Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view," *International Journal of Modern Education and Computer Science*, vol. 12, no. 6, pp. 29–45, 2020, doi: 10.5815/ijmecs.2020.06.03.

[8] S. Sruthy, S. Yamuna, and S. N. George, "An IoT based active building surveillance system using raspberry Pi and NodeMCU," 2020, [Online]. Available: http://arxiv.org/abs/2001.11340.

[9] F. I. Sangkop *et al.*, "Web based home automation system prototype using Raspberry Pi," pp. 292-297, 2020, doi: 10.5220/0009010002920297.

[10] G. Sairam, K. Prabhas, S. Ahammad, A. Varshith, and R. Santhoshkumar, "Secure enterprise networking with blockchain-enabled zero trust access control systems," *Int. J. Eng. Res. Sci. Technol.*, vol. 22, no. 2–3, pp. 350–357, 2026.

[11] M. J. Nur, D. R. I. M. Setiadi, A. A. Ojugo, and M. T. Nguyen, "Improving customer churn prediction using domain-driven feature engineering, resampling, and CatBoost with explain ability extensions," *Proceedings - 2025 International Seminar on Application for Technology of Information and Communication: Advancing Electrical Engineering and Informatics Through Quantum Computing and Intelligence Technologies, iSemantic 2025*, pp. 493–499, 2025, doi: 10.1109/ISemantic67418.2025.11291801.

[12] F. S. Perilla, G. R. Villanueva, N. M. Cacanindin, and T. D. Palaoag, "Fire safety and alert system using arduino sensors with IoT integration," *ACM International Conference Proceeding Series*, pp. 199–203, 2018, doi: 10.1145/3185089.3185121.

[13] C. Stolojescu-Crisan, C. Crisan, and B. P. Butunoi, "An IoT-based smart home automation system," *Sensors*, vol. 21, no. 11, 2021, doi: 10.3390/s21113784.

[14] B. Sarwar, I. S. Bajwa, N. Jamil, S. Ramzan, and N. Sarwar, "An intelligent fire warning application using IoT and an adaptive neuro-fuzzy inference system," *Sensors (Switzerland)*, vol. 19, no. 14, 2019, doi: 10.3390/s19143150.

[15] A. H. Allam, I. Gomaa, H. H. Zayed, and M. Taha, "IoT-based eHealth using blockchain technology: a survey," *Cluster Computing*, vol. 27, no. 6, pp. 7083–7110, 2024, doi: 10.1007/s10586-024-04357-y.

[16] B. O. Malasowe, F. O. Aghware, M. D. Okpor, E. B. Edim, R. E. Ako, and A. A. Ojugo, "Techniques and best practices for handling cybersecurity risks in educational technology environment (EdTech)," *NIPES - Journal of Science and Technology Research*, vol. 6, no. 2, pp. 293–311, 2024, doi: 10.5281/zenodo.12617068.

[17] N. A. Azeez, K. M. Adeleke, T. G. Fadara, and O. B. Ologunye, "Development and Implementation of an IoT-Based smart door control system for enhanced security and remote access," *1st Int. Conf. Eng.*, vol. 1, no. April, pp. 7–9, 2025.

[18] S. N. Okofu *et al.*, "Pilot study on consumer preference, intentions and trust on purchasing-pattern for online virtual shops," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 7, pp. 804–811, 2024, doi: 10.14569/IJACSA.2024.0150780.

[19] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, "A comparative analysis of supervised machine learning algorithms for IoT attack detection and classification," *Journal of Computing Theories and Applications*, vol. 2, no. 3, pp. 395–409, 2025, doi: 10.62411/jcta.11901.

[20] B. O. Malasowe, M. I. Akazue, E. A. Okpako, F. O. Aghware, A. A. Ojugo, and D. V. Ojie, "Adaptive learner-CBT with secured fault-tolerant and resumption capability for Nigerian universities," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, pp. 135–142, 2023, doi: 10.14569/IJACSA.2023.0140816.

[21] W. J. Sheng, I. F. Kasmin, S. Amin, and N. K. Zainal, "Addressing user perception and implementing Hedera Hashgraph and voice recognition into multi-factor authentication (MFA) system," *International Journal of Data Science and Advanced Analytics*, vol. 4, pp. 194–201, 2023, doi: 10.69511/ijdsaa.v4i0.165.

[22] E. Marasco, M. Albanese, V. V. R. Patibandla, A. Vurity, and S. S. Sriram, " Biometric multi-factor authentication: On the usability of the FingerPIN scheme ," *Security and Privacy*, vol. 6, no. 1, 2023, doi: 10.1002/spy2.261.

[23] F. O. Aghware *et al.*, "Effects of data balancing in diabetes mellitus detection: a comparative XGBoost and random forest learning approach," *NIPES - Journal of Science and Technology Research*, vol. 7, no. 1, pp. 1–11, 2025, doi: 10.37933/nipes/7.1.2025.1.

[24] S. David, "ArcFace-Based retinal biometric access control system with arduino-servo door mechanism and esp32 iot integration," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 14, no. 5, pp. 2144–2150, May 2026, doi: 10.22214/ijraset.2026.81386.

[25] A. P. Binitie, S. I. Onyemenem, N. C. Anujeonye, A. A. Ojugo, F. A. Egbokhare, and T. C. Aghaunor, "A graph-augmented isolation forest using Node2Vec and GraphSAGE for mobile user behavior anomaly detection," *Journal of Computing Theories and Applications*, vol. 3, no. 3, pp. 369–383, 2026, doi: 10.62411/jcta.15494.

[26] M. I. Akazue *et al.*, "Handling transactional data features via associative rule mining for mobile online shopping platforms," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 3, pp. 530–538, 2024, doi: 10.14569/IJACSA.2024.0150354.

[27] C. E. Hou, R. Sliusar, A. Ghauforian, T. Makanju, and U. Zakia, "A hybrid edge-cloud smart door surveillance system with real-time risk assessment and secure access control," *2025 IEEE 16th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2025*, pp. 630–637, 2025, doi: 10.1109/IEMCON67450.2025.11381064.

[28] H. L. Labaran, U. Shehu Muhammad, U. S. Umar, M. E. Rana, and A. S. Daradara, "Design and development of an intelligent access control system using real-time facial recognition for smart door automation," *2025 IEEE 1st Int. Conf. Emerg. Innov. Digit. Technol. ICEIDT 2025*, pp. 92–97, 2025, doi: 10.1109/ICEIDT66693.2025.11473431.

[29] F. M. Sarimole, S. W. Yudha, Sutisna, and R. A. Akmal, "Implementation of an RFID card based automatic door lock system using nodemcu with integration of telegram notifications and IoT services," *Int. J. Appl. Math. Comput.*, vol. 2, no. 4, pp. 16–23, 2025, doi: 10.62951/ijamc.v2i4.126.

[30] H. Li, X. Yang, H. Wang, W. Wei, and W. Xue, "A controllable secure blockchain-based electronic healthcare records sharing scheme," *Journal of Healthcare Engineering*, vol. 2022, 2022, doi: 10.1155/2022/2058497.

[31] B. Leiding and A. Norta, "Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10646 LNCS, pp. 181–196, 2017, doi: 10.1007/978-3-319-70004-5_13.

[32] C. Nartey *et al.*, "On blockchain and IoT integration platforms: current implementation challenges and future perspectives," *Wireless Communications and Mobile Computing*, vol. 2021, 2021, doi: 10.1155/2021/6672482.

[33] I. Ehsan *et al.*, "Internet of things-based fire alarm navigation system: a fire-rescue department perspective," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/3830372.

[34] D. Sun, M. Liu, M. Li, Z. Shi, P. Liu, and X. Wang, "DeepMIT: a novel malicious insider threat detection framework based on recurrent neural network," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, IEEE, May 2021, pp. 335–341. doi: 10.1109/CSCWD49262.2021.9437887.

[35] L. He, C. Ma, C. Tu, and Y. Zhang, "Gait2Vec: continuous authentication of smartphone users based on gait behavior," *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2022*, pp. 280–285, 2022, doi: 10.1109/CSCWD54268.2022.9776313.

[36] A. O. Eboka *et al.*, "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 (IJ-ICT)*, vol. 14, no. 1, pp. 287–297, Apr. 2025, doi: 10.11591/ijict.v14i1.pp287-297.
[37] A. Mohd Ibrahim, I. Venkat, P. De Wilde, M. R. Mohd Romlay, and A. Bahamid, "The role of crowd behavior and cooperation strategies during evacuation," *Simulation*, vol. 98, no. 9, pp. 737–751, 2022, doi: 10.1177/00375497221075611.
[38] S. Kanagamalliga, S. Rajalingam, A. Kannan, and M. Karthikeyan, "Biometric and IoT integration for secure and remote door access control using fingerprint recognition and GSM technology," *E3S Web of Conferences*, vol. 619, 2025, doi: 10.1051/e3sconf/202561903013.
[39] P. D. Karningsih, R. Kusumawardani, N. Syahroni, Y. Mulyadi, and M. S. B. M. Saad, "Automated fish feeding system for an offshore aquaculture unit," *IOP Conference Series: Materials Science and Engineering*, vol. 1072, no. 1, p. 012073, 2021, doi: 10.1088/1757-899x/1072/1/012073.
[40] S. A. Salloum, K. M. Alomari, A. M. Alfaisal, R. A. Aljanada, and A. Basiouni, "Emotion recognition for enhanced learning: using AI to detect students' emotions and adjust teaching methods," *Smart Learning Environments*, vol. 12, no. 1, 2025, doi: 10.1186/s40561-025-00374-5.
[41] S. H. T. Hussien, L. Vinukumar, C. H. C. Alexander, and S. Sivakumar, "Smart campus attendance and security systems: Leveraging IoT for enhanced efficiency," *AIP Conf. Proc.*, vol. 020153, 2024, doi: 10.1063/5.0229386
[42] Safuan *et al.*, "Transformer-based support for content-validity pre-screening in educational materials," *Journal of Computing Theories and Applications*, vol. 4, no. 1, pp. 423–442, Aug. 2026, doi: 10.62411/jcta.16829.
[43] J. J. D. Rivera, A. Muhammad, and W. C. Song, "Securing digital identity in the zero-trust architecture: a blockchain approach to privacy-focused multi-factor authentication," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2792–2814, 2024, doi: 10.1109/OJCOMS.2024.3391728.
[44] K. Okeke and S. Omojola, "Enhancing cybersecurity measures in critical infrastructure: challenges and innovations for resilience," *Journal of Scientific Research and Reports*, vol. 31, no. 2, pp. 474–484, 2025, doi: 10.9734/jsrr/2025/v31i22868.
[45] S. Sruthy, S. Yamuna, and S. N. George, "An IoT based active building surveillance system using Raspberry Pi and NodeMCU," Jan. 2020.
[46] T. C. Aghaunor *et al.*, "Investigating security enhancement in hybrid clouds via a blockchain-fused privacy preservation strategy: pilot study," *J. Comput. Theor. Appl.*, vol. 3, no. 4, pp. 428–442, 2026, doi: 10.62411/jcta.15508.
[47] M. Ohemu and M. O. Idoko, "Development of a low-cost IoT-enabled door access control system for smart home security," *Asian J. Comput. Sci. Technol.*, vol. 14, no. 2, pp. 43–50, 2025, doi: 10.70112/ajcst-2025.14.2.4387.
[48] J. J. Diaz Rivera, T. A. Khan, W. Akbar, A. Muhammad, and W.-C. Song, "Secure enrollment token delivery for zero trust networks using blockchain," in *2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Sep. 2022, pp. 1–6, doi: 10.23919/APNOMS56106.2022.9919940.
[49] Azhari, R. R. Manullang, M. Yanti, C. D. Hasibuan, and E. Yudhistira, "Performance of secure door access system using identification numbers, fingerprints, and facial recognition," *J. Phys. Conf. Ser.*, vol. 2733, no. 1, pp. 1–10, 2024, doi: 10.1088/1742-6596/2733/1/012003.
[50] J. Singh, C. Patel, and N. K. Chaudhary, "Resilient risk-based adaptive authentication and authorization (RAD-AA) framework," Nov. 2022, [Online]. Available: http://arxiv.org/abs/2208.02592.
[51] D. R. I. M. Setiadi *et al.*, "Hyperchaotic cross-coupled quantum 2D maps with interdependent rotational asymmetry for secure image encryption," *Optics Communications*, vol. 600, 2026, doi: 10.1016/j.optcom.2025.132699.
[52] R. Karanjai *et al.*, "Decentralized translator of trust: supporting heterogeneous TEE for critical infrastructure protection," pp. 85–94, 2023, doi: 10.1145/3594556.3594626.
[53] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: protecting users from credit-card fraud transaction via the deep-learning cluster ensemble," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 94–100, 2023, doi: 10.14569/IJACSA.2023.0140610.
[54] Y. Watanabe and L. Kun, "Long-term influence of user identification based on touch operation on smart phone," *Procedia Computer Science*, vol. 112, pp. 2529–2536, 2017, doi: 10.1016/j.procs.2017.08.196.
[55] N. J. Gandrathi, V. Thaduka, A. Suram, S. V. Konda, and G. Thotakuri, "Intelligent lock system with facial recognition and fingerprint-based authentication applications," *International Journal of AI Electronics and Nexus Energy*, vol. 2, no. 2, pp. 255–261, 2026, doi: 10.64751/4qf11v82.
[56] S. Akshith, R. Mukka, A. Karthik, S. Krishna V, J. F. G. Poovathy, and I. Divya, "IoT-enabled multi-factor authentication lock system," *Journal of Information System and Technology Management*, vol. 10, no. 39, pp. 197–208, 2025, doi: 10.35631/jistm.1039013.
[57] A. E. Ibor, E. B. Edim, and A. A. Ojugo, "Secure health information system with blockchain technology," *Journal of the Nigerian Society of Physical Sciences*, vol. 5, no. 2, 2023, doi: 10.46481/jnsps.2023.992.
[58] A. E. Ibor, D. U. Ashishie, J. A. Odey, B. I. Ele, and A. A. Ojugo, "Can we unchain the blockchain? a review of attacks on elliptic curve cryptography and countermeasures," *Security and Privacy*, vol. 9, no. 4, 2026, doi: 10.1002/spy2.70234.
[59] X. Jin and K. Omote, "An efficient blockchain-based authentication scheme with transferability," *PLoS ONE*, vol. 19, no. 9 September, 2024, doi: 10.1371/journal.pone.0310094.
[60] R. E. Yoro *et al.*, "Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner," *Plos One*, vol. 20, no. 6 June, 2025, doi: 10.1371/journal.pone.0326571.
[61] D. Kafetzopoulos, C. Stylios, and D. Skalkos, "Managing traceability in the meat processing industry: Principles, guidelines and technologies," in *CEUR Workshop Proceedings*, 2020, vol. 2761, pp. 302–308.
[62] R. Halder, D. Das Roy, and D. Shin, "A blockchain-based decentralized public key infrastructure using the web of trust," *Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 196–222, 2024, doi: 10.3390/jcp4020010.
[63] A. Bouras, I. Khalil, and B. Aouni, "Blockchain driven supply chains and enterprise information systems," *Blockchain Driven Supply Chains and Enterprise Information Systems*, pp. 1–222, 2022, doi: 10.1007/978-3-030-96154-1.
[64] N. Afrin and A. Pathak, "Blockchain-powered security and transparency in supply chain: exploring traceability and authenticity through smart contracts," *International Journal of Computer Applications*, vol. 185, no. 49, pp. 5–15, 2023, doi: 10.5120/ijca2023923318.
[65] D. R. I. M. Setiadi *et al.*, "Single qubit quantum logistic-sine XYZ-rotation maps: an ultra-wide range dynamics for image encryption," *Comput. Mater. Contin.*, vol. 83, no. 2, pp. 2161–2188, 2025, doi: 10.32604/cmc.2025.063729.
[66] H. H. Ou, C. H. Pan, Y. M. Tseng, and I. C. Lin, "Decentralized identity authentication mechanism: integrating FIDO and blockchain for enhanced security," *Applied Sciences (Switzerland)*, vol. 14, no. 9, 2024, doi: 10.3390/app14093551.
[67] H. Fereidooni *et al.*, "AuthentiSense: a scalable behavioral biometrics authentication scheme using few-shot learning for mobile platforms," *30th Annual Network and Distributed System Security Symposium, NDSS 2023*, 2023, doi: 10.14722/ndss.2023.23194.

BIOGRAPHIES OF AUTHORS



Andrew Okonji Eboka received his HND in Computer Science from the Akanu Ibiam Federal Polytechnic, Ebonyi State in 1998; PGD from the Ebonyi State University in 2013, B.Sc./Ed in Computer Science Education from the Enugu State University of Science and Technology in 2013. He received M.Sc. in Network Computing from Coventry University, United Kingdom. He is a Chief Lecturer at the Federal College of Education Technical Asaba, Nigeria. His research interests include: cybersecurity, ubiquitous computing, and forensics. He is a member of: The British Computer Society, Association of Computer Machinery, Computer Professionals of Nigeria and International Association of Engineers. He can be contacted at email: andrew.eboka@fcetasaba.edu.ng.



Fidelis Obukohwo Aghware received BSc in Computer Science from The University of Benin in 1998; MSc in 2005 from the Nnamdi Azikiwe University Awka, and also Ph.D. in Computer Science in 2015 from The Ebonyi State University, Abakiliki. He is currently an Associate Professor with the Department of Computer Science, Uniiversity of Delta in Agbor, Delta State of Nigeria. His interests include: CyberSecurity, Data Science and Information Technology. He is a member of Nigerian Computer Society, the Council for Registration of Computer Professionals of Nigeria, and the International Association of Engineers. He can be contacted at email: fidelis.aghware@unidel.edu.ng.



Margaret Dumebi Okpor received her B.Sc. and M.Sc. in Computer Science from the University of Benin, Nigeria in 1997 and 2014 respectively. She further proceeded to obtain her Ph.D. in Computer Science from the Ignatius Ajuru University of Education in Rivers State. She currently lectures with the Department of Computer Science at The Delta State University of Science and Technology Ozoro in Delta State; and here research interest includes (but not limited to): machine intelligence, data science, and cybersecurity. She is a member of Nigerian Computer Society and Council of Computer Professionals of Nigeria (CPN). She can be contacted at email: okpormd@sdu.edu.ng.



Bridget Ogheneovo Malasowe received her B.Sc. and M.Sc. in Computer Science from the University of Benin in Edo State in 1997 and 2014 respectively. She further proceeded to obtain her Ph.D. in Computer Science from the Ignatius Ajuru University of Education in Rivers State. She currently lectures with the Department of Computer Science at The Delta State University of Science and Technology Ozoro in Delta State; and here research interest(s) includes (but not limited to): machine intelligence, data science, and cybersecurity. She is a member of Nigerian Computer Society and Council of Computer Professionals of Nigeria (CPN). She can be contacted at email: okpormd@sdu.edu.ng.



Ejaita Abugor Okpako received BSc, MSc and Ph.D. (Computer Science) from the University of Port Hàrcourt, Nigeria. He is presently aan Associate Professor and the Dean, Faculty of Computing at the University of Delta, Agbor, Nigeria. His interest include Artificial Intelligence, Data Science, Cyber Security, Big Data, Software Engineering. He served previously as the Director of ICT, Edwin Clark University, Kiagbodo, Delta State, Nigeria. He has published various articles in both referred Journals and Conference proceedings. He can be contacted at email: ejaita.okpako@unidel.edu.ng.



Arnold Adimabua Ojugo received his BSc Computer Science from Imo State University Owerri in 2000; MSc Computer Science from Nnamdi Azikiwe University Awka in 2005, and Ph.D. Computer Science from the Ebonyi State University Abakiliki in 2013. He currently lectures with the Department of Data Science, at the Federal University of Petroleum Resource Effurun, Nigeria. His interest includes: Intelligent Systems, Machine Learning, Cybersecurity, and Graph Connectionist. He is affiliated with: Nigerian Computer Society, Computer Professionals of Nigeria, and The International Association of Engineers. He is an Editor of Sustainable Computing, Informatics and Systems and other Scopus Indexed Journals. Married to Dr. Theresa Nkem Ojugo, they have six (6) children: Gregory, Easterbell, Emmanuel, Eric, Elena and Elizabeth. He can be contacted at email: ojugo.arnold@fupre.edu.ng.



Reuben Akporube Abere received his BSc Computer Science, M.Sc Computer Science and Ph.D. Computer Science – all from the University of Benin, Nigeria in 1999, 2006 and 2026 respectively. He is currently a Senior Lecturer with the Department of Computer Science, Federal University of Petroleum Resources Effurun, Nigeria. His interests include: Software Engineering: Model Construction and User Trust Systems, Mobile Telecommunication, Information Technology, and Computer Architecture & Organization. He is a member of American Computing Machinery. He can be contacted at email: abere.reuben@fupre.edu.ng.



Amaka Patience Binitie obtained her BSc degree in Computer Science from Nnamdi Azikiwe University Awka, Nigeria, in 2007. She obtained her MSc degree in Computer science from Adamawa State University, Nigeria in 2015 and her Ph.D. in computer from the University of Benin, Nigeria in 2023. She is currently a lecturer at the Federal College of Education Technical Asaba. She has lots of publications to her name. Her research interests are in the areas of Cyber Security, Information Technology, and Artificial Intelligence. She can be contacted at email: amaka.binitie@fcetasaba.edu.ng.



Rita Erhovwo Ako received her B.Sc. Industrial Mathematics degree from Delta State University, Abraka, Delta State, Nigeria in 2000; M.Sc. Computer Science from the University of Ibadan, Oyo State, Nigeria in 2005; M.Sc. Internet, Computer and System Security and Ph.D. Computer Science from the University of Bradford, Bradford, United Kingdom in 2006 and 2013 respectively. She is currently a senior lecturer with the Department of Computer Science at The Federal University of Petroleum Resources Effurun. She has several publications to her credit with research interests in: artificial intelligence, cybersecurity, e-commerce, embedded systems, and risk management. She is a member of the Nigerian Computer Society. She can be contacted at email: ako.rita@fupre.edu.ng.



Innocent Sunny Onyemenem received his B.Sc. Computer Science from the University of Nigeria Nssukka in 20026; MSc in Info Technology from the University of Aberdeen in 2022. He currently lectures with the Department of Computer Science at The Federal College of Education (Technical) Asaba in Nigeria. He has several publications to his credit with research interests in: Information Technology, Cybersecurity, e-commerce, and risk management. He is a member of the Nigerian Computer Society and the Council for the Registration of Computer Professionals in Nigeria. He can be contacted at email: innocentsunnyonyemenem@gmail.com.



Adesuwa Inaya is a Lecturer in Computer Science at Federal College of Education Technical, Asaba, Delta State. She holds an MSc in Computer Science from Chukwuemeka Odumegwu Ojukwu University and a BSc in Computer Science from the Ambrose Alli University, Ekpoma in Nigeria. She is currently a Ph.D. candidate at Chukwuemeka Odumegwu Ojukwu University and a TRCN certified educator. Her research interests are in Artificial Intelligence and Computer Science. She is a member of NCS and TRCN. She can be contacted at email: debbietupsy@yahoo.co.uk.



Victor Ochuko Geteloma received his B.Sc. in Computer Science from the Federal University of Petroleum Resources Effurun, Delta State, Nigeria in 2015; M.Sc. in Computer Science in 2019 from the Covenant University, Ogun State. He is currently undergoing his Doctoral Studies, and currently lectures with the Department of Computer Science at the Federal University of Petroleum Resources Effurun. He has several publications to his credit. His research interests include: Cybersecurity, Cloud computing, e-Government, Technology Adoption, and Digital Inclusion. He is a member of the Nigerian Computer Society. He can be contacted at email: geteloma.victor@fupre.edu.ng.