

International Journal Research Publication Analysis

Page: 01-17

DESIGN AND IMPLEMENTATION OF A SECURE MOBILE-BASED DIGITAL DOCUMENT SIGNING AND VERIFICATION SYSTEM

***Okonkwo, I. B., Umeh, M. N., Okonkwo, I. G.**

Nigeria.

Article Received: 24 August 2026

*Corresponding Author: Okonkwo, I. B.

Article Revised: 12 September 2026

Nigeria.

Published on: 02 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.3101>

ABSTRACT

The increasing use of electronic documents across educational institutions, government agencies, corporate organizations and other sectors has intensified the need for mechanisms capable of guaranteeing document authenticity, integrity and accountability. Conventional electronic document management systems remain vulnerable to forgery, unauthorized modification, identity impersonation and weak access control. This study presents TrustSign, a secure Android-based digital document signing and verification system developed to address these challenges through the integration of multiple security mechanisms. The system combines One-Time Password (OTP) and biometric fingerprint authentication, Role-Based Access Control (RBAC), RSA digital signatures, SHA-256 hashing, Android Keystore-based key management, QR-code verification, Firebase cloud storage, audit trails and verification logs. The system was designed using Object-Oriented Analysis and Design Methodology and implemented using Java and Android Studio. Firebase Realtime Database was used for user information, document metadata, audit records and verification logs, while Firebase Storage was used for signed PDF documents. Functional testing was conducted using valid and invalid credentials, biometric data, PDF documents, QR codes and different user roles. Results showed that all major functional modules passed their tests. The system successfully authenticated users, enforced role-based permissions, digitally signed documents, generated unique TrustSign identification numbers and QR codes, verified authentic documents, detected modified documents, and maintained audit and verification records. The study demonstrates that integrating strong authentication, cryptographic signatures, access control, cloud services and verification mechanisms within a mobile platform provides a practical approach to secure digital document management.

KEYWORDS: Digital document, digital signature, mobile security, RSA, SHA-256, biometric authentication, RBAC, QR code, TrustSign.

1. INTRODUCTION

The rapid adoption of digital technologies has transformed the creation, transmission, storage and management of documents. Organizations increasingly depend on electronic documents because they provide faster access, easier distribution, lower storage requirements and improved administrative efficiency. However, the movement from physical to electronic documents has also introduced security challenges associated with document forgery, unauthorized modification, identity impersonation, unauthorized access and weak accountability.

Electronic documents are particularly vulnerable when organizations rely primarily on passwords and conventional document-management mechanisms. Compromised credentials may allow unauthorized persons to gain access to sensitive information, while inadequate document-integrity mechanisms may make it difficult to determine whether a document has been altered after its creation or approval. These challenges are particularly important for documents whose authenticity carries administrative, financial, academic or legal significance.

Authentication provides the first layer of protection by establishing the identity of users before access is granted. However, conventional password-based authentication may be inadequate where sensitive information and critical operations are involved. Multi-factor authentication provides additional assurance by combining independent authentication factors. In the TrustSign system, authentication is strengthened through One-Time Password (OTP) and biometric fingerprint verification. The implemented system sends an OTP to the user's registered phone and subsequently performs fingerprint authentication through the Android Biometric Authentication API.

Authentication, however, does not determine the activities that an authenticated user is allowed to perform. This requires authorization. Role-Based Access Control (RBAC) addresses this concern by assigning permissions according to predefined roles. TrustSign implements three principal roles: Administrator, Auditor and General User. Each role receives a different set of system privileges.

Another major requirement is the ability to establish document authenticity and integrity. Digital signatures provide cryptographic evidence associated with the signer, while hashing allows a system to determine whether the contents of a document have changed. TrustSign

combines RSA digital signatures with SHA-256 hashing. A hash is generated for each document before signing, while a new hash is generated during verification and compared with the stored value to identify modification. RSA is used to generate and verify the digital signature.

Recent studies have addressed different aspects of authentication, access control and document security. Kumar et al. (2025), for example, combined multimodal authentication with RBAC but did not integrate digital signatures for data verification. Vijjapu et al. (2024) integrated RBAC, RSA and digital signatures in a healthcare system, but relied primarily on conventional authentication. Other studies have investigated blockchain-based access control, attribute-based access control and extended RBAC without providing a unified combination of strong authentication, RBAC and digital signatures.

The literature therefore indicates a gap in the holistic integration of secure authentication, RBAC and digital signatures across user roles and system interactions. The present study addresses this gap through the development of TrustSign, a mobile-based platform that combines authentication, authorization, cryptographic signing, document verification, QR-code technology, cloud storage and audit logging within a unified system.

The main objective of the study was to design and implement a secure mobile-based digital document signing and verification system. Specifically, the study sought to:

1. Implement secure user authentication using otp and biometric fingerprint verification;
2. Implement rbac for controlling user privileges;
3. Implement rsa-based digital signatures and sha-256 hashing for document security;
4. Provide secure cloud-based storage for documents and metadata;
5. Implement qr-code-based document identification and verification; and
6. Maintain audit trails and verification logs for accountability and traceability.

The contribution of the study is a practical mobile security architecture that integrates identity verification, role-based authorization and cryptographic document authentication within one operational platform.

2.0 RELATED LITERATURE

2.1 Digital Document Security

Digital document security involves mechanisms for protecting electronic documents against unauthorized access, modification, forgery and repudiation. Unlike physical documents, electronic documents can be copied and modified without obvious physical evidence of

alteration. Consequently, digital document-management systems require mechanisms capable of establishing document provenance and detecting unauthorized changes. Digital signatures provide one of the principal cryptographic mechanisms for addressing these requirements. A digital signature links a document to a cryptographic private key associated with the signer, while the corresponding public key enables verification. Hashing complements digital signatures by producing a fixed-length representation of document contents.

In TrustSign, SHA-256 is used to generate document hashes and RSA is used to create digital signatures. During verification, the system generates a new hash and compares it with the stored hash while also verifying the RSA signature.

2.2 Multi-Factor Authentication

Authentication establishes whether a person requesting access to a system is an authorized user. Password-only mechanisms may be compromised through credential theft, phishing and other attacks. Multi-factor authentication improves security by requiring more than one authentication factor.

TrustSign combines OTP and fingerprint authentication. The OTP provides a temporary authentication credential sent to the registered phone, while fingerprint verification provides a biometric factor linked to the authorized device user.

This approach is particularly relevant to digital document signing because unauthorized access to the signing function could allow an attacker to generate apparently legitimate documents.

2.3 Role-Based Access Control

RBAC provides a structured method for managing authorization. Instead of assigning permissions independently to every user, privileges are assigned to roles and users are assigned appropriate roles.

TrustSign implements three roles. Administrators have broad system privileges, Auditors have access to verification and monitoring functions, and General Users are restricted primarily to their own document operations.

The use of RBAC therefore provides an additional security layer after authentication by ensuring that successful authentication does not automatically provide unrestricted access.

2.4 Cryptographic Key Management

Digital-signature systems depend heavily on the protection of private cryptographic keys. If a private signing key is compromised, an unauthorized individual could potentially generate signatures associated with the legitimate user.

TrustSign uses the Android Keystore System for RSA key generation and management. The private key remains protected within the device's secure environment rather than being exposed to users or external applications.

2.5 Cloud-Based Document Storage

Cloud computing provides scalable infrastructure for storing documents and associated metadata. TrustSign uses Firebase Realtime Database and Firebase Storage. The actual signed PDF documents are stored in Firebase Storage, while associated information—including document identifiers, signatures, hashes, public keys, timestamps and status—is maintained in Firebase Realtime Database. This separation allows the system to manage document files and structured metadata independently while maintaining a centralized verification environment.

2.6 QR-Code-Based Verification

QR codes provide a convenient mechanism for connecting physical or electronic documents to digital verification records. In TrustSign, each signed document receives a unique TrustSign identification number and QR code. The QR code can subsequently be scanned to retrieve the corresponding document information and verification result.

2.7 Related Empirical Studies and Research Gap

Recent studies demonstrate growing interest in combining authentication and access-control technologies. Kumar et al. (2025) investigated multimodal authentication and RBAC but did not integrate digital signatures. Mohamed et al. (2025) developed a containerized attribute-based access-control system without digital signatures for non-repudiation. Adhithiyan (2025) examined blockchain and RBAC for healthcare records but did not apply digital signatures to user actions.

Vijjapu et al. (2024) represents one of the closest related studies because it combined RBAC, RSA and digital signatures in a healthcare environment. However, the system relied on basic authentication and lacked strong multi-factor authentication. The literature reviewed in the complete study therefore identifies a gap in systems that simultaneously integrate secure authentication, RBAC and digital signatures across user roles and interactions. TrustSign was developed to address this gap.

3.0 METHODOLOGY

3.1 Research and Development Approach

The study adopted Object-Oriented Analysis and Design Methodology (OOADM). The methodology was considered appropriate because TrustSign is object-oriented and contains

identifiable entities, users, documents, roles, authentication processes and system interactions. OOADM also supports the use of UML-based modelling and promotes modularity, maintainability, scalability and code reuse. The development process involved:

1. Analysis of the existing system;
2. Identification of functional and security requirements;
3. System modelling and design;
4. Implementation of the proposed system;
5. Integration of security mechanisms; and
6. Functional testing and evaluation.

3.2 Existing-System Analysis

The existing system examined in the study was the Medicare web application developed by Vijjapu et al. (2024). The system combined RBAC, AES encryption, RSA digital signatures, session management and MongoDB in a healthcare environment. Although the existing approach demonstrated the usefulness of combining access control and cryptographic protection, the study identified limitations in authentication and broader integration. These limitations informed the development of TrustSign.

3.3 System Requirements

The requirements of TrustSign were derived from the identified security gap. The system was required to support:

- Secure user registration;
- Otp authentication;
- Biometric authentication;
- Role-based authorization;
- Pdf document signing;
- Document verification;
- Qr-code generation and scanning;
- Cloud-based storage;
- Audit logging; and
- Verification logging.

4.0 SYSTEM DESIGN

4.1 Overall System Architecture

TrustSign was designed as a modular Android-based system. The principal user categories are Administrator, Auditor and General User. After authentication, each user is directed to a dashboard containing only the functions permitted by the assigned role.

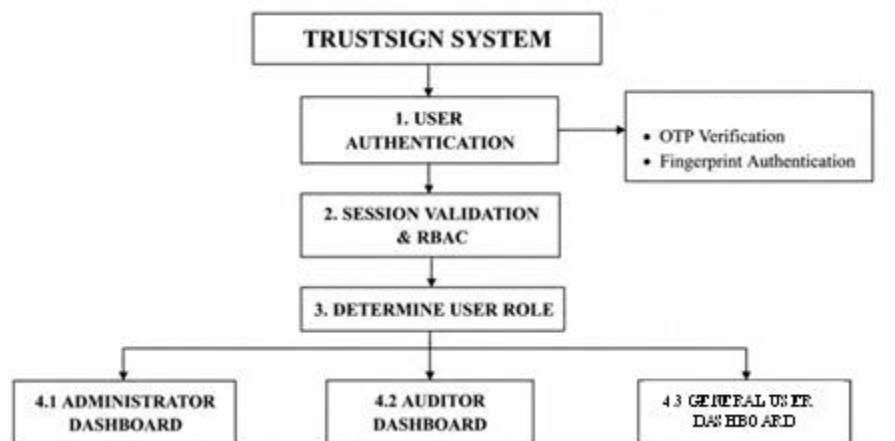


Figure 1. High-Level Architecture and User-Access Flow of the TrustSign System.

4.2 Role-Based Access Control Design

The system uses RBAC to separate user privileges. The Administrator has the broadest access, including user registration and management, document signing and verification, QR-code scanning, audit trails and reports. The Auditor has access to verification, QR scanning, audit activities and document viewing, while the General User has access to document signing, verification, QR scanning and personal document management.

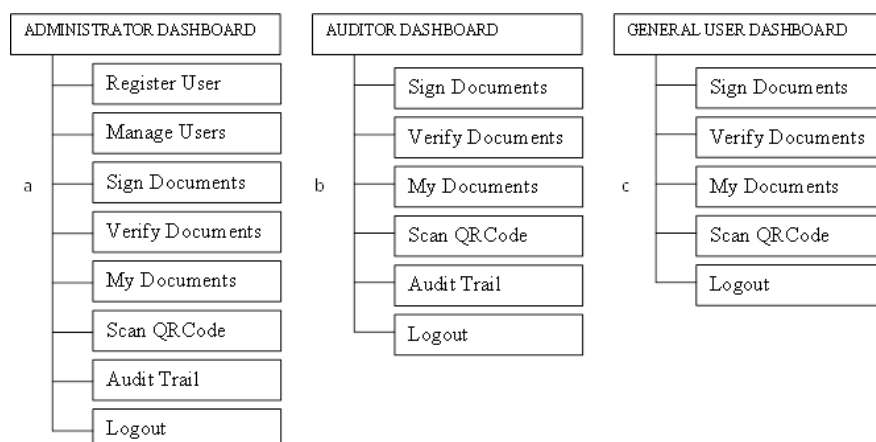


Figure 2. Role-Based Dashboards of the TrustSign System: (a) Administrator, (b) Auditor, and (c) General User.

4.3 Cloud Architecture

TrustSign uses Firebase as its cloud infrastructure. Firebase Authentication supports authentication, Firebase Realtime Database maintains structured application information and Firebase Storage stores signed PDF documents.

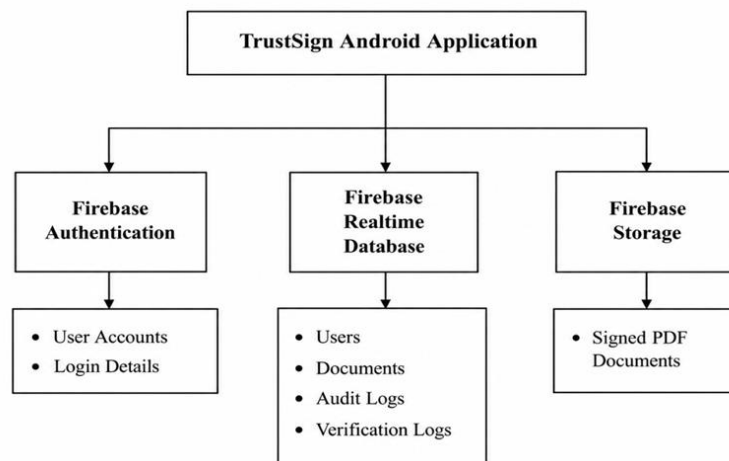


Figure 3. Cloud-Based Architecture of the TrustSign System.

4.4 Digital Document Signing and Verification Workflow

The document-signing process begins when an authorized user selects a PDF document. The system generates a SHA-256 hash, creates an RSA digital signature using the protected private key, uploads the signed document to Firebase Storage and stores the associated metadata in Firebase Realtime Database. A unique TrustSign identification number and QR code are also generated.

During verification, the system generates a new hash from the document and compares it with the stored hash. The RSA signature is also verified using the corresponding public key. A mismatch indicates that the document has been altered.



Figure 4. Digital Document Signing and Verification Workflow in TrustSign.

5.0 SYSTEM IMPLEMENTATION

5.1 Application Development Environment

TrustSign was implemented as an Android application. Java and Android Studio were used for application development, while Firebase services provided the cloud backend. The implementation incorporates RSA and SHA-256 for cryptographic operations, Android Keystore for key protection and QR-code technology for document identification and verification.

5.2 Authentication Implementation

The authentication module uses OTP followed by fingerprint authentication. After successful authentication, the system identifies the user's role and directs the user to the appropriate dashboard. The implementation procedure requires the user to launch the application, enter the registered phone number, receive and enter an OTP, complete fingerprint authentication and access the role-specific dashboard.

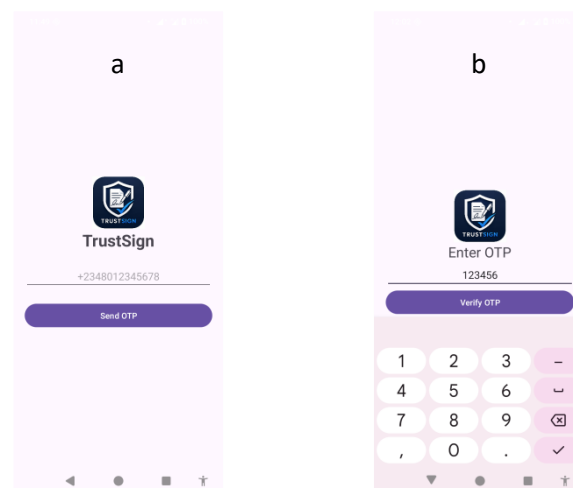


Figure 5. TrustSign Multi-Factor Authentication Interfaces: (a) Login and (b) OTP Verification.

5.3 Digital Document Signing

The document-signing module allows authorized users to select a PDF document and initiate the signing process. The system generates a SHA-256 hash and RSA digital signature, uploads the signed document to Firebase Storage, generates a QR code and stores document information in Firebase Realtime Database.

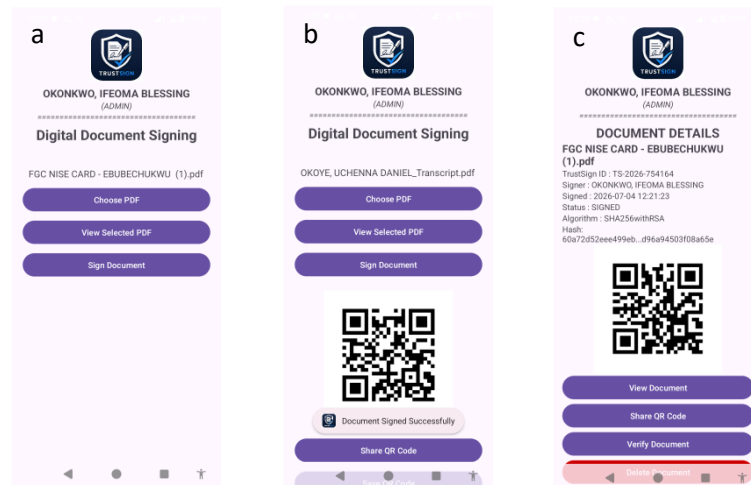


Figure 6. TrustSign Digital Document Signing Interface and Generated Verification Identity: (a) PDF Selection/Signing, (b) Successful Signing, and (c) TrustSign ID and QR Code.

5.4 Document Verification

The verification module validates both the document hash and the RSA digital signature. A document that has not been altered should produce a matching hash and valid signature, whereas a modified document should fail the integrity check.

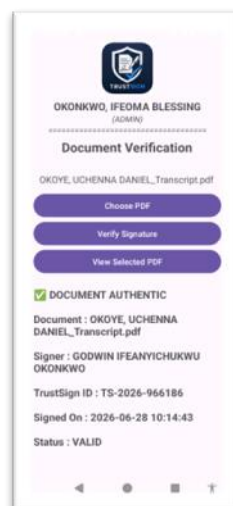


Figure 7. Digital Document Verification Results: Authentic Document Successfully Verified.

5.5 QR-Code Verification

TrustSign generates a QR code associated with each digitally signed document. The QR-code verification function enables users to scan the code and retrieve the associated document

information. The General User interface, for example, provides a dedicated Scan QR Code function that retrieves document information from the database and verifies its authenticity.

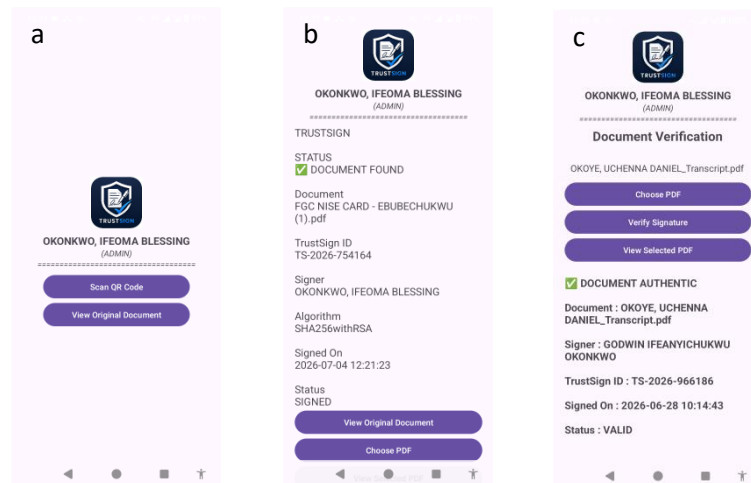


Figure 8. QR-Code-Based Document Verification: (a) QR-Code Scanner, (b) Retrieved Document Information, and (c) Verification Result.

5.6 Audit Trail and Verification Logging

TrustSign maintains an audit trail to record significant system activities. These include user registration, document signing, document verification, QR-code verification, document viewing and document deletion. Verification logs separately maintain the history and outcome of document verification activities.

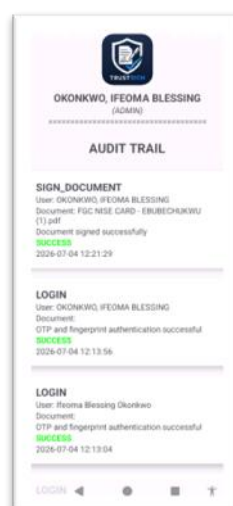


Figure 9. TrustSign Accountability Interface: Audit Trail.

6.0 TESTING AND EVALUATION

6.1 Functional Testing

The system was tested using valid and invalid user credentials, valid and invalid OTP values, registered and unregistered fingerprints, sample PDF documents, original and modified PDF documents, valid and invalid QR codes, and Administrator, Auditor and General User accounts. The functional testing covered ten major modules:

1. User Authentication;
2. User Registration;
3. Role-Based Access Control;
4. Document Signing;
5. Document Verification;
6. QR-Code Verification;
7. My Documents;
8. Audit Trail;
9. Verification Logs; and
10. Document Management.

Table 1. Functional Test Results.

S/N	Test Module	Expected Result	Actual Result	Status
1	User Authentication	Access after successful OTP and fingerprint verification	Users authenticated and redirected to appropriate dashboards	Pass
2	User Registration	User information stored	User details stored successfully	Pass
3	RBAC	Users access only assigned functions	Appropriate dashboard and permissions displayed	Pass
4	Document Signing	PDF digitally signed and uploaded	PDF signed, uploaded and assigned TrustSign ID and QR code	Pass
5	Document Verification	Authentic documents verified	Original documents verified; modified documents detected	Pass
6	QR-Code Verification	QR code retrieves document information	Correct document information retrieved	Pass
7	My Documents	User documents displayed	Signed documents displayed successfully	Pass
8	Audit Trail	Activities recorded	User activities successfully logged	Pass
9	Verification Logs	Verification records stored	Verification history successfully recorded	Pass
10	Document Management	Authorized users manage documents	Documents managed according to privileges	Pass

Source: Adapted from the completed TrustSign system testing results.

All major functional modules passed their specified tests. The document-verification test was particularly significant because original documents were successfully verified while modified documents were detected.

6.2 Performance Evaluation

The completed study evaluated the system in terms of functionality, response time, reliability, security, usability and scalability.

The functional results indicate that the implemented system performed according to its specified requirements. The successful execution of authentication, authorization, signing, verification, QR-code processing, document management and logging demonstrates that the major components operated as intended.

However, the evaluation should be interpreted as a **functional system evaluation**, rather than as evidence of large-scale enterprise deployment. The system was evaluated within the development/testing environment, and therefore broader deployment studies would be required to establish performance under large concurrent workloads.

6.3 Security Evaluation

The security architecture operates through multiple complementary layers. OTP and fingerprint authentication protect user access; RBAC controls authorization; SHA-256 provides document-integrity checking; RSA provides digital signatures; Android Keystore protects cryptographic keys; Firebase Security Rules protect cloud resources; and audit and verification logs support accountability. This layered architecture reduces dependence on any single security mechanism.

7.0 DISCUSSION

The findings demonstrate the feasibility of integrating multiple security mechanisms within a single mobile-based digital document management system.

The successful authentication results indicate that OTP and biometric verification can be combined to strengthen access to sensitive document functions. Rather than relying solely on a password or other single credential, TrustSign introduces additional verification before users reach their authorized dashboards.

The successful RBAC tests further demonstrate that authentication and authorization serve different but complementary purposes. Authentication establishes the identity of the user,

while RBAC determines which functions that authenticated user may access. The three role-specific dashboards provide a visible implementation of this distinction.

The digital-signature results provide the strongest evidence of document security. The system successfully signed PDF documents and assigned them unique TrustSign identification numbers and QR codes. During verification, original documents were successfully authenticated while modified documents were detected.

This result is important because document security should not be limited to controlling who can access a document. A secure system must also provide mechanisms for determining whether the document itself has remained unchanged. The combination of SHA-256 hashing and RSA signatures provides this capability.

The Android Keystore component further strengthens the system by protecting private signing keys within the device's secure environment. This is important because the compromise of a private key could undermine the authenticity of documents signed by the corresponding user. The implemented design keeps the private key protected and uses the corresponding public key for verification.

The QR-code component provides an additional practical advantage. Conventional digital verification may require users to manually locate document records or enter identification information. By associating each signed document with a QR code, TrustSign provides a direct mechanism through which document information can be retrieved and verified.

The audit trail and verification logs also contribute to accountability. Recording significant activities allows system administrators and auditors to determine what activities occurred and provides a historical record of verification events. This is particularly important in organizational environments where documents may need to be traced after issuance or verification.

The results are broadly consistent with the gap identified in the literature. Previous studies have addressed multimodal authentication, RBAC, blockchain-based access control and digital signatures, but the literature reviewed in the study identified a lack of unified systems integrating secure authentication, RBAC and digital signatures across user roles and interactions.

TrustSign therefore contributes an integrated architecture in which: *Authentication* → *Authorization* → *Digital Signing* → *Document Verification* → *QR Verification* → *Auditability* operate as connected components rather than isolated security mechanisms.

Nevertheless, the findings should not be overstated. Successful functional testing does not establish that the system is completely immune to cyberattacks. Large-scale penetration

testing, independent security auditing, load testing and real-world organizational deployment would provide stronger evidence of security and scalability.

8.0 CONCLUSION

This study presented the design and implementation of TrustSign, a secure mobile-based digital document signing and verification system developed to improve the authenticity, integrity, security and accountability of electronic documents.

The system integrates OTP and biometric fingerprint authentication, RBAC, RSA digital signatures, SHA-256 hashing, Android Keystore, QR-code verification, Firebase cloud storage, audit trails and verification logs. These mechanisms provide multiple layers of protection covering user identity, authorization, document integrity, cryptographic authenticity, storage and accountability.

The functional evaluation demonstrated successful performance across all ten major modules tested. Users were authenticated successfully, role-specific access was enforced, PDF documents were digitally signed, TrustSign IDs and QR codes were generated, original documents were verified, modified documents were detected, and audit and verification records were maintained.

The study therefore concludes that integrating strong authentication, role-based authorization and cryptographic document verification within a mobile platform provides a practical approach to secure electronic document management. The system has potential application in educational institutions, government agencies, corporate organizations and other environments where document authenticity and traceability are important.

Future studies should evaluate TrustSign under real-world organizational conditions and investigate broader security testing, larger workloads, additional document formats, cross-platform implementation, offline verification and other advanced technologies.

REFERENCE

1. Adhithyan, E. (2025, June 8). Secure health record storing using blockchain with role-based access control [Preprint]. SSRN. <https://doi.org/10.2139/ssrn.5313917>
2. Ferdous, M. S. (2024, December 1). A blockchain and capability-based access control for Internet of Things using self-sovereign identity.
3. <https://dspace.bracu.ac.bd/xmlui/handle/10361/25529>
4. Kumar, C. K., Sunil, C., Swarup, B. R. N., Afroz, P. S., Saileela, B., & Banu, S. S. (2025, March). A sophisticated authentication coupled with a multimodal security

- integration and role-based access control for secure file management. In *2025 5th International Conference on Expert Clouds and Applications (ICOECA)* (pp. 192–202). IEEE.
5. Mohamed, S. I., Mostafa, M., Assaly, J., & Shalabi, A. S. (2025). Containerized attribute-based access control system using digital keys. *Deleted Journal*. <https://doi.org/10.1007/s43995-025-00149-6>
 6. Morrison, D. (2023). *Development of a secure, role-based password manager*. <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3078086>
 7. Pradhan, G., & Priyadarsini, M. (2024). A trusted computing framework for cloud data security using role-based access and pattern recognition. *Cluster Computing*, 27(5), 6609–6622. <https://doi.org/10.1007/s10586-024-04274-0>
 8. Shi, W. (2024). *Extended role-based access control model for enterprise systems and web services*. Figshare. <https://doi.org/10.25439/rmt.27339978>
 9. Sutradhar, S., Karforma, S., Bose, R., Roy, S., Djebali, S., & Bhattacharyya, D. (2023). Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A blockchain-based approach for security and scalability for healthcare industry. *Internet of Things and Cyber-Physical Systems*, 4, 49–67. <https://doi.org/10.1016/j.iotcps.2023.07.004>
 10. Vijjapu, A., Alagawadi, A. P., Maddi, A., & Kavitha, C. R. (2024). Enhancing medical record security: Using role-based access control, digital signatures, and RSA encryption. In *2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 484–488). <https://doi.org/10.1109/ICECA63461.2024.10800884>
 11. Zaidi, T., Usman, M., Aftab, M. U., Aljuaid, H., & Ghadi, Y. Y. (2023). Fabrication of flexible role-based access control based on blockchain for Internet of Things use cases. *IEEE Access*, 11, 106315–106333. <https://doi.org/10.1109/ACCESS.2023.3318487>
 12. Al-Haj, A., & Al-Tamimi, A. (2022). Secure digital signature schemes for mobile devices: A review and new directions. *Journal of King Saud University – Computer and Information Sciences*, 34(10), 8821–8837.
 13. Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two-factor authentication using mobile phones. In *IEEE/ACS International Conference on Computer Systems and Applications* (pp. 641–644). <https://doi.org/10.1109/AICCSA.2009.5069395>

14. Chen, S., Li, Z., Fan, L., & Zhang, Y. (2023). Security analysis of Android Keystore implementations. *IEEE Transactions on Dependable and Secure Computing*, 20(4), 2981–2996.
15. Ferraiolo, D. F., Kuhn, R. D., & Chandramouli, R. (2003). *Role-based access control*. Artech House.
16. National Institute of Standards and Technology. (2013). *Digital Signature Standard (DSS) (FIPS PUB 186-4)*. U.S. Department of Commerce.
<https://doi.org/10.6028/NIST.FIPS.186-4>
17. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1), Article 1.
18. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2), 38–47. <https://doi.org/10.1109/2.485845>