International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

SecureVault

Anil Raut[1], Glory Lithiyal[2], Dr. Rakhi O. Gupta[3], Nashrah Gowalker[4]

[1,2]Department of Information Technology, Kishinchand Chellaram College, HSNC University, Mumbai, India

[3]Co-Ordinator, I.T Department Kishinchand Chellaram College, HSNC University, Mumbai, India

[4]Assistant Professor, I.T. Department, Kishinchand Chellaram College, HSNC University, Mumbai, India

Abstract

In today's digital world, protecting sensitive information is essential. This project creates a Secure Document Management System that uses encrypted QR codes to store and verify business credentials. Employees scan their official documents, which are then encrypted and stored in QR codes. These documents are uploaded to the system and can only be accessed by authorized personnel through decryption in a custom app, preventing standard QR code scanners from accessing the data.

The system combines encryption, QR code generation, and secure storage to create a tamper-proof solution for managing sensitive documents. It ensures data privacy, compliance with security policies, and protection against unauthorized access, maintaining the integrity of employee records and providing a secure method for document verification.

Keywords: Secure Document Management Encrypted QR Codes, Data Privacy, Document Verification, Role-Based Access Control, Multi-Factor Authentication, AES/RSA Encryption, Secure Storage, Custom Software Application, Sensitive Information Protection

I. INTRODUCTION

In the digital age, managing and protecting sensitive information has become paramount for organizations. The rise of cyber threats, data breaches, and the increasing volume of personal and confidential data that organizations handle, make it more crucial than ever to ensure secure storage and verification of such information. One of the primary challenges organizations face is maintaining the integrity and confidentiality of employee credentials, personal records, and other important documents. These documents must be easily accessible by authorized personnel while protected from unauthorized access, alteration, or misuse.

To address these challenges, the SecureVault system has been developed as a Secure Document Management System that utilizes encrypted QR codes to safely store and verify important documents. The system works by scanning official documents, encrypting them, and embedding them into QR codes, which are then uploaded to the system. This ensures that even if the QR code is intercepted, the information remains encrypted and unreadable to unauthorized individuals. Only authorized personnel with access to a custom decryption method can unlock and access the encrypted data, preventing unauthorized access. This mechanism ensures that only those with the correct credentials and permissions can view or modify sensitive documents.

The use of encrypted QR codes within SecureVault not only provides a robust level of security but also makes document verification more efficient. Employees and organizations can quickly scan QR codes for document validation without the need for traditional, often cumbersome, verification processes. Moreover, SecureVault's design incorporates role-based access control (RBAC) and multi-factor authentication (MFA) to further enhance security. These features ensure that only individuals with the appropriate permissions can access or alter sensitive documents, adding a layer of protection against internal and external threats.

This paper explores how SecureVault presents a scalable and secure solution to the ongoing problem of safeguarding sensitive organizational data. It highlights the integration of modern encryption techniques, secure storage mechanisms, and the use of QR code technology as an innovative method for document verification. Additionally, the research discusses how SecureVault can help organizations comply with data privacy regulations and security policies while simplifying the document management process. The ultimate goal of SecureVault is to provide a tamper-proof, efficient, and easily scalable system for managing sensitive information, ensuring data privacy, and preventing unauthorized access in an increasingly digital world.

II. LITERATURE REVIEW

The need for secure document management has increased significantly due to the rise in cyber threats and the growing reliance on digital systems. This section reviews existing research and technological approaches that have influenced the development of SecureVault.

A. Secure Document Management Systems

Existing document management systems prioritize data storage and access control but often fall short in implementing end-to-end security measures. Studies highlight the use of encryption as a primary defense against unauthorized access. However, traditional systems rely heavily on centralized storage, which is prone to single points of failure. Encrypted QR codes have emerged as a novel approach, allowing secure, portable data that can be accessed only by authorized users with specific decryption mechanisms.

B. Encryption Techniques

Encryption algorithms like Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) are widely acknowledged for their robustness. AES is highly efficient for symmetric key encryption, making it suitable for large-scale data encryption, while RSA provides secure asymmetric encryption for transmitting sensitive keys. Combining these techniques ensures both high security and operational efficiency.

C. Role-Based Access Control (RBAC)

RBAC is a well-researched access control mechanism that limits access based on user roles. Studies have shown its effectiveness in minimizing insider threats by ensuring that only designated personnel can access specific resources. Multi-factor authentication (MFA) further strengthens RBAC by requiring an additional verification step, reducing the risk of unauthorized access.

D. QR Code Applications in Security

Recent advancements in QR code technology have enabled their application in secure data storage and retrieval. Encrypted QR codes are increasingly being used in industries such as healthcare and finance for secure information sharing. Research demonstrates their potential to ensure data integrity while maintaining ease of access for authorized personnel.

E. Comparison with Existing Solutions

SecureVault differentiates itself from existing systems by integrating encrypted QR codes with a proprietary decryption application. Unlike conventional systems, which rely on static passwords or public QR codes, SecureVault uses advanced encryption to ensure data privacy even if the QR code is intercepted. This approach addresses vulnerabilities in traditional systems while offering scalability and compliance with privacy regulations.

III METHODOLOGIES

A. System Architecture

1. **Document Encryption:** Documents are converted into secure encrypted QR codes using a combination of AES (for symmetric encryption) and RSA (for key exchange). This ensures robust protection against unauthorized access during storage and transmission.
2. **Role-Based Access Control (RBAC):** Access to documents is restricted based on the user's role within the organization. This ensures that only designated personnel can view or manage specific encrypted data.
3. **Multi-Factor Authentication (MFA):** To enhance security, MFA requires users to authenticate using two or more verification methods, such as passwords and one-time codes.
4. **Decryption Process:** The proprietary software ensures that only authorized personnel using the SecureVault application can decrypt the QR codes. Standard QR scanners cannot read these codes, adding a layer of security.

B. Workflow

1. **Document Upload:** Employees upload official credentials to the system, where they are encrypted into QR codes.
2. **Admin Management:** Admins manage these encrypted credentials through a centralized web-based dashboard, ensuring streamlined handling and storage.
3. **Verification Process:** Using the SecureVault app, authorized personnel decrypt and verify the data embedded in QR codes for organizational purposes.

IV. OBJECTIVE OF THE STUDY

A. **Secure Storage of Documents:** To utilize encrypted QR codes for storing sensitive employee and business-related credentials, ensuring robust protection against unauthorized access.

B. **Enhanced Authentication Mechanisms:** To implement multi-factor authentication (MFA) and role-based access control (RBAC) to ensure that only authorized personnel can access and manage sensitive data.

C. **Streamlined Verification Process:** To create a centralized web interface for admins to manage encrypted credentials and an organizational app for efficient decryption and verification.

D. **Scalability and Compliance:** To ensure the system is scalable and adheres to data privacy regulations, making it suitable for organizations of various sizes and industries.

E. **User-Friendly and Tamper-Proof Solution:** To provide an easy-to-use system that simplifies document verification while maintaining high standards of security and data integrity.

VI. CONCLUSION

The SecureVault system provides a robust and scalable solution to the challenges of secure document management in the digital era. Integrating encrypted QR codes, advanced encryption techniques like AES and RSA, and multi-factor authentication, ensures that sensitive documents are protected from unauthorized access. The system's user-friendly interface and role-based access control further enhance its usability and operational efficiency, making it suitable for organizations of all sizes across various industries. With its strong focus on security and compliance with data privacy regulations, SecureVault offers a reliable framework for managing sensitive credentials.

Looking ahead, SecureVault has the potential to evolve with the integration of technologies such as blockchain for immutable audit trails and AI for proactive threat detection. These advancements would further bolster its security and adaptability. By continuously addressing emerging security challenges and user needs, SecureVault can establish itself as a leading solution for document management, setting new benchmarks in security, efficiency, and scalability.

VII. FUTURE WORK

The SecureVault system has demonstrated its effectiveness in secure document management through encrypted QR codes and advanced authentication mechanisms. However, there are several opportunities for improvement and expansion to enhance its functionality and adaptability.

A. **Integration with Blockchain Technology:** Implementing blockchain for immutable audit trails can ensure transparent and tamper-proof logging of all document access and verification activities, further enhancing security and trust.

B. **Artificial Intelligence for Anomaly Detection:** Incorporating AI algorithms to monitor access patterns and detect anomalies can proactively identify potential threats or unauthorized access attempts.

C. **Cross-Platform Compatibility:** Extending the system to support a wider range of devices, including seamless integration with mobile platforms and wearable technology, would improve accessibility and usability.

D. **Real-Time Monitoring and Alerts:** Adding features for real-time monitoring of document access and instant notifications for unauthorized attempts could strengthen security protocols.

E. **Enhanced User Experience:** Developing intuitive user interfaces and incorporating natural language processing (NLP) for voice commands could make the system more user-friendly and accessible to a broader audience.

F. **Scalability for Larger Organizations:** Optimizing the system's architecture to support large-scale deployments, including integration with cloud storage and enterprise resource planning (ERP) systems, would cater to the needs of multinational corporations.

G. **Regulatory Compliance Upgrades:** Updating the system to align with evolving data privacy and security regulations, such as GDPR, CCPA, and HIPAA, would ensure broader applicability across industries.

VIII. ACKNOWLEDGMENT

We would like to take this opportunity to express a deep sense of gratitude to Dr. Tejashree V. Shanbhag (Principal of K.C. College) and Dr. Rakhi Gupta (H.O.D. of B.Sc. I.T. Department) for their cordial support, valuable information and guidance, which helped us in completing this task through various stages. We take this opportunity to express our profound gratitude and deep regards to our guides, Dr. Rakhi Gupta, and Mrs. Nashrah Gowalker for their exemplary guidance, monitoring, and constant encouragement throughout this project. The blessing, help, and guidance given by her from time to time shall carry us a long way in the journey of life on which we are about to embark.

We are obliged to staff members of K.C. College for the valuable information provided by them in their respective fields. We are grateful for their cooperation during the period of our project.

IX. REFERENCES

1. **Sharma, Rahul, and Pooja Verma.** "Multi-Level Encryption System Using AES and RSA Algorithms." *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 10, no. 5, May 2022, www.ijraset.com/research-paper/multi-level-encryption-system-using-aes-and-rsa-algorithms.
2. **"AES vs. RSA Encryption: What Are the Differences?"** *Precisely*, 3 Mar. 2022, www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences.
3. **"Encrypted QR Code: A Complete Guide with Best 6 Advantages."** *Scanova Blog*, 12 July 2023, scanova.io/blog/encrypted-qr-code.
4. **DigiDoc Technologies.** "Leveraging Multi-Factor Authentication, Encryption, and Access Control in Document Management Systems." *DigiDoc Technologies Blog*, July 2024, www.digidoc.tech/blog/multi-factor-authentication-encryption-access-control.
5. **QRLab.** "QR Codes for Secure Document Sharing and Verification." *QRLab Blog*, 2023, qrlab.com/blog/post/qr-codes-for-secure-document-sharing-and-verification.
6. **"Streamlining Document Management with QR Codes."** *QR Codes Australia Blog*, 2023, qrcodesaustralia.com.au/document-management-with-qr-codes.
7. **"Encryption and Access Control."** *FasterCapital*, 2024, fastercapital.com/topics/encryption-and-access-control.html.
8. **"Top 5 Methods of Protecting Data."** *TitanFile Blog*, 15 Mar. 2024, www.titanfile.com/blog/5-methods-of-protecting-data.
9. **"File Management System: Tracking File-Document with RFID & QR Code."** *Ruddersoft Blog*, July 2024, www.ruddersoft.com/blog/1042-file-management-system-tracking-file-document-with-rfid-qr-code