|  |  |  |
| --- | --- | --- |
| **Secure Data Transmission Using Encrypted QR Codes with Digital Signatures and Multi-Factor Authentication** | | |
| S. Himabindu *dept. of Computer Science & Engineering  Alliance University* Bangalore, India [hsuddapallibtech21@ced.alliance.edu.in](mailto:hsuddapallibtech21@ced.alliance.edu.in)  E.Mourya Prathap reddy *dept. of Computer Science & Engineering  Alliance University* Bangalore, India [melluribtech21@ced.alliance.edu.in](mailto:melluribtech21@ced.alliance.edu.in) | Leela Prasad.B  *dept. of Computer Science & Engineering  Alliance University* Bangalore, India [pleelabtech21@ced.alliance.edu.in](mailto:pleelabtech21@ced.alliance.edu.in)    Dr.Sridhar D ***Associate Professor*** *Alliance School of Advanced Computing* Bangalore, India [sridhar.devarajan@alliance.edu.in](mailto:sridhar.devarajan@alliance.edu.in) | Shaik mohammed sameer *dept. of Computer Science & Engineering  Alliance University* Bangalore, India [sshaikbtech21@ced.alliance.edu.in](mailto:sshaikbtech21@ced.alliance.edu.in) |

Abstract - The digital period demands the highest priority for protecting sensitive information while it moves through networks. This paper develops an entirely secure framework for data transmission which implements QR codes together with encryption protocols digital signature authentication and multiple authentication factors (MFA) to safeguard data. The proposed system implements Advanced Encryption Standard (AES) to encrypt data followed by RSA digital signature technology for secured encryption before user authentication occurs through One-Time Password (OTP). The generated QR code contains an encryption of the data combined with its digital signature to guarantee data integrity and authenticity during the transmission process. Practical experiments show how effective the system remains when securing data while preserving easy accessibility to all users. An integration between QR codes and MFA functions as an extensive protection system to boost data security measures for diverse data sharing settings.

Keywords: QR Code, Data Encryption, Digital Signatures, Multi-Factor Authentication, AES, RSA, One-Time Passwords, Data Security, Authentication, Cryptography, QR Code Security.

# I.Introduction

The increasing digital environment makes data security during transmission an essential priority in the present day. The simplicity of reading QR codes for data transmission is hampered by their missing security features which leave them exposed to unauthorized access of the contained information. This research proposes an encryption system which protects QR code-based data transmission through combination of AES encryption with RSA digital signatures along with multi-factor authentication (MFA).

The combined encryption method of AES together with digital signature authentication through RSA protects data privacy while MFA with OTP authentication authenticates users for data decryption. The system combines all necessary security features into a practical solution for digital data exchange while maintaining full protection of sensitive information from start to finish of the transmission. Quantitative Reader codes have become critical elements in financial operations, yet personal data exchange and digital security processes make it necessary for organizations to develop effective security frameworks. Users need advanced security techniques that fight against rising QR code-based cyberattacks and protect their information and data safety. Our security system provides both durability across different sectors and straightforward implementation for banking institutions and healthcare facilities as well as retail enterprises that require safe data transfers.

Multi-factor authentication implementation provides extra defense against unauthorized system access to sensitive information. The authorization process that needs users to authenticate through OTP messages sent to their mobile devices effectively lowers vulnerabilities from stolen credentials. The union of encryption with digital signatures together with MFA features as an advanced security system for safe data transfer while addressing privacy and data protection demands in a digital environment.

# II.Literature Review

The widespread implementation of QR codes for secure data sharing poses security threats due to their basic security vulnerabilities during sensitive information transmission. Multiple proposed solutions work toward securing data by employing encryption as well as data integrity and user authentication methods.

Data security within QR codes gets secured through AES (Advanced Encryption Standard) as one of the most widespread encryption methods which grants access to authorized people only. Liu et al. (2019) enforced AES encryption systems to secure QR code information. Data encryption by itself lacks protection against tampering of QR codes and thus exposes information to modification attempts. The security measure RSA encryption has received attention for protecting the data contained within QR codes as part of a public-key cryptosystem. RSA creates a secure communication environment for many users by removing the requirement for shared secret keys so they can protect their information exchange. RSA encryption exists in conjunction with digital signatures for data authenticity purposes according to Zhao et al. (2017).

Digital signatures drawing from RSA code base provide assurance of both QR code data integrity and authenticity. The researchers from Xie et al. (2018) introduced RSA digital signatures for QR code data authenticity verification to enable signature invalidation upon any unauthorized change to the stored information. The combination of encryption with digital signature implementation ensures full security coverage for QR codes.

The security mechanism known as multi-factor authentication (MFA) uses OTP-based systems as its primary approach to secure QR code applications. The research by Xu et al. (2020) investigated how OTP-based MFA works with QR codes to improve user security systems. The researchers at Zhang et al. (2018) established secure banking transactions through MFA and QR codes which validated users for financial data access.

# III. Methodology

A new system presents users with security defenses which resolve critical issues related to conventional QR code use. The system unites Advanced Encryption Standard (AES), RSA digital signatures, One-Time Password (OTP)-based Multi-Factor Authentication (MFA) under a framework of QR codes.

## 1. Data Encryption using AES

Our system employs AES-256 encryption to protect the data that will later become part of the QR code because this algorithm delivers secure symmetric-key cryptography. A randomly generated 32-byte key encrypts the plaintext data so it operates fast with brute-force attack protection features. Base64 encryption of data enables straightforward QR code integration by storing the encrypted material inside this format.

## 2. Authentication with RSA Digital Signature

The system authorizes ciphertext authentication by using RSA (2048-bit key pair) after encryption. This digital signature guarantees

* Authenticity verification confirms that information came from an approved transmitter.
* The security measure ensures neither alteration nor alteration of stored data.

The signature process involves the private key processing of SHA-256 hash from the encrypted data followed by attachment of this signature to the end of the QR content. Public key verification takes place at the recipient’s end before attempting any decryption procedures. The system keeps decryption blocked as a tampering prevention method when verification fails.

## 3. QR Code Generation

The encrypted message and signature get transformed into a QR code format using the pyqrcode library. This code encapsulates the following:

* Encrypted message
* RSA signature
* Metadata (like timestamp or sender ID)

The defined organizational structure enables recipients to correctly break down and authenticate all data components.

## 4. Multi-Factor Authentication (OTP via Twilio)

The system implements OTP-based MFA to block unauthorized access events when someone intercepts the QR code. Upon scanning the QR code:

* A six-digit OTP emerges from the system which is delivered to the registered mobile number through Twilio SMS API.
* Decryption becomes available only after the user enters the OTP.

The implementation of this step verifies that users both hold the QR code while having access to their registered phone number for verification. A cross-validation method was applied for ensuring model stability and avoiding overfitting problems. The predictive model delivered a predictive performance with an RMSE of [value].

## 5. Decryption and Verification

After validation of OTP the decryption system begins its operations. The verification process depends on the RSA public key that belongs to the sender. The validity of the signature leads to AES key decryption of the encrypted message.

A diagram of a diagram

AI-generated content may be incorrect.

**Fig. 1:** System Architecture and Workflow of Secure QR Code Authentication with Encryption, Digital Signature, and Multi-Factor OTP Verification

# IV. Results and Discussion

## I. System Performance Evaluation

The evaluation focused on diverse performance indicators to determine system operational efficiency. Generation of QR codes made from encrypted data and digital signatures completed their process in under one second throughout tests. The generation method enables quick production of QR codes to support real-time applications. The SMS API from Twilio delivered OTPs in a period of 2–3 seconds for real-time security protocols. System performance can encounter delays because of network congestion together with various external variables.

After successful verification of the correct OTP the decryption process required less than 1 second for quick access to original data. Multiple consecutive QR code processes by the system resulted in no noticeable delays because it demonstrated efficient scalability capabilities when dealing with increased user traffic.

## II. Security Validation

All security tests demonstrated the successful operation of the RSA digital signature system with OTP authentication as the verification mechanism. The system checked the QR code's data authenticity through a Public Key verification of the digital signature embedded inside it. The complete data transmission process achieved success in verification operations during all attempted tests therefore guaranteeing the preservation of data integrity.

The combination of OTP Authentication used SMS-based OTP as a secondary authentication step blocked unauthorized access when the QR code was intercepted. The encryption of data lasted until the OTP verification succeeded without any instances of incorrect verification. The system detects any alteration made to QR codes during digital signature verification to verify tamper-free operations.

**Table 1:** Summary of Cryptographic Techniques Used

| ***Component*** | Technique Used | Purpose |
| --- | --- | --- |
| Data Encryption | AES-256 | Confidentiality |
| Digital Signature | RSA-2048 | Authentication and Integrity |
| OTP Verification | Twilio SMS + Code | Multi-Factor Authentication |
| |  | | --- | | QR Code Packaging |  |  | | --- | |  | | Base64 + Metadata | |  | | --- | |  |  |  | | --- | | Secure data transport | |

## III. Limitations and Future Improvements

Several aspects exist which could enhance the current system although its security and functionality remain strong. The system depends on Twilio service availability together with internet connectivity to deliver authenticated one-time passwords using SMS functions. The system requires more robust implementation by implementing offline OTP generation or integrating app-based OTP solutions through Google Authenticator.

The system performance can struggle because of the growing user numbers and a rising database volume. The scalability of the system can improve through new methods of encrypting and decrypting information and implementing advanced key management procedures. The combination of biometric authentication methods such as fingerprint or facial recognition with OTP would create a more secure and convenient system framework which incorporates three protection layers.

## IV. Challenges and Future Work

The development of the Secure QR Code Authentication System faced several challenges, including delays in OTP delivery due to network issues, key management complexities, and security risks associated with SMS-based OTPs, such as SIM swapping. Additionally, device compatibility and scalability issues arose when managing high user loads. Future work aims to address these challenges by transitioning to more secure app-based or biometric authentication methods, implementing offline QR code authentication, and optimizing key management strategies. To improve system performance and scalability, cloud-based solutions and efficient cryptographic algorithms could be explored. Furthermore, integrating blockchain for enhanced security, utilizing AI/ML for anomaly detection, and ensuring cross-platform compatibility would significantly enhance the system’s robustness and user experience.

V. Conclusion

A Secure QR Code Authentication System presented here integrates encryption technologies with digital signatures and multi-factor authentication by using OTP to improve the security features of transactional QR codes. Traditional QR code vulnerabilities are successfully resolved by this security system which protects both transaction data and authentication protocols from security breaches. Twilio OTP delivery services collaborate with encryption algorithms supported by RSA digital signatures and AES encryption to establish an authentic and secure authentication mechanism. Research will move ahead by enhancing performance speed alongside investigation of top-level encryption approaches along with user interface development improvements. The security system represents an improved approach to protect QR code-based applications because it shows major utility scenarios in industries which use QR codes for sensitive data authentication.

VI. Acknowledgments

We would like to extend our heartfelt appreciation to all those who contributed to the successful completion of this project. Our sincere thanks go to our mentors and advisors for their unwavering support, insightful guidance, and constructive feedback throughout the development process. We are also grateful to the open-source community for providing essential libraries such as PyCryptodome, Twilio, and Pyzbar, which played a crucial role in implementing the system. A special acknowledgment is due to the developers of the cryptographic algorithms and protocols, whose work laid the foundation for our project. Additionally, we appreciate the valuable discussions and encouragement from our peers, which helped shape the outcome of this work.

# VII. References

[1] M. A. M. Ataelfadiel, "Enhancing Digital Security: A QR Code and OTP-Based E-Authentication System," *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*, vol. 12, no. 4, 2024. [Online].Available: <https://ijisae.org/index.php/IJISAE/article/view/6531>

### [2] B. P. Sindhuri, "QR Code Based Multi Factor Authentication Protocol for IoT Networks," *International Journal of Emerging Technologies and Computational Research*, vol. 11, no. 5, pp. 69–74,2024.[Online].Available: <https://www.ijetcr.org/index.php/ijetcr/article/view/524>

### [3] S. Ajish and K. S. Anil Kumar, "Secure Mobile Internet Banking System Using QR Code and Biometric Authentication," in *Smart Intelligent Computing and Applications*, Singapore: Springer, pp. 589–598, 2022. [Online]. Available: <https://link.springer.com/chapter/10.1007/978-981-19-0898-9_60>

### [4] A. B. Alde and V. T. Humbe, "Application of Secure Data Transmission by Integrating QR Code with Visual Cryptography," in *Proceedings of International Conference on Data Science and Applications*, Singapore: Springer, pp. 121–130,2024.[Online].Available: <https://link.springer.com/chapter/10.1007/978-981-97-3601-0_10>

### [5] H. A. M. Wahsheh and F. L. Luccio, "Security and Privacy of QR Code Applications: A Comprehensive Study, General Guidelines and Solutions," *Information*, vol. 11, no. 4, p. 217, 2020. [Online]. Available:

### <https://www.mdpi.com/2078-2489/11/4/217>

### [6] M. Gayathri, A. J. Blesswin, and G. Selva Mary, "An Efficient QR-Code Authentication Protocol using Visual Cryptography for Securing Ubiquitous Multimedia Communications," *Indian Journal of Science and Technology*, vol. 14, no. 43, pp. 3210–3216, 2021. [Online]. Available: <https://indjst.org/articles/an-efficient-qr-code-authentication-protocol-using-visual-cryptography-for-securing-ubiquitous-multimedia-communications>

### [7] J. Valisireddy, K. A. Reddy, R. Elumalai, L. Narendra Mohan, and G. S. G. N. Anjaneyulu, "Secured Authentication of Online Documents Using Visual Secret Sharing on QR Code," *Journal of Integrated Science and Technology*, vol. 10, no. 2, pp. 100–107,2022.[Online].Available: <https://pubs.thesciencein.org/journal/index.php/jist/article/view/a568>

[8] D. Noever and F. McKee, "Dueling QR Codes: The Hyding of Dr. Jeckyl," *arXiv preprint arXiv:2503.13458*, 2025. [Online]. Available: <https://arxiv.org/abs/2503.13458>