Enhancing Security and Efficiency through QR Integration with Hybrid AES-ECC Algorithm in Mobile Apps for Cardless Data Transactions

Noor J. Hamad[*], Abbas A. Abdulhameed[**], Mudhafar H. Ali[***]

[*] College of Engineering, Al-Iraqia University, Iraq
Email: noorjhy@gmail.com
https://orcid.org/0009-0009-4550-3297

[**]Computer Science, University of Mustansiriyah, Iraq
Email: abbasabdulazeez@uomustansiriyah.edu.iq
https://orcid.org/0000-0002-1132-2756

[***] College of Engineering, Al-Iraqia University, Iraq
Email: mudhafar.ali@aliraqia.edu.iq
https://orcid.org/ 0000-0001-8447-5502

Abstract

To improve and facilitate transactions between customers and financial institutions, the utilization of Internet banking has been leveraged to deliver a heightened caliber of service characterized by heightened security and efficiency in contrast to traditional banking modalities. It is suggested in this research introduces an innovative security framework, designed to furnish a protected mechanism ensuring secure communication, authentication, confidentiality, and safeguarding of financial transactions between banking institutions and end-users, all without necessitating reliance on a physical card. The fundamental underpinning of this proposed system involves the amalgamation of a Quick Response (QR) code with a hybridized Advanced Encryption Standard-Elliptic Curve Cryptography (AES-ECC) model. Following the successful installation of the security application on the mobile device, and subsequent to an accomplished registration and encryption of data inputs, encoding and decoding processes are facilitated through the intrinsic encoding and decryption keys embedded within this hybrid algorithm. The clientele receives a QR code containing encrypted transaction details, and upon scanning this code via the designated Android application, the pertinent information is promptly displayed. Empirical assessments validate the effectiveness of the suggested approach, demonstrating superior outcomes when juxtaposed with prevailing methodologies.

Keywords- AES, Authentication, Decryption, ECC, Encryption, QR Code.

I. INTRODUCTION

Mobile banking has become a preferred method due to mobile technology adoption. It offers cost-effective, high-quality services with the potential for location-based features. Compared to Internet banking, it's more user-friendly and secure, providing 3A convenience (anytime, anywhere, anyhow). Its availability and efficiency drive customer adoption [1]. Despite the advantages of online banking, it faces challenges from cybercrime. Phishing, fraud, and breaches erode trust in financial institutions. Security is crucial, necessitating secure transactions and robust systems. To counter ATM threats, cardless ATMs via Android apps are used, yet criminals modify apps to steal login data. Online transaction security is now vital due to breaches and theft, harming trust, and transactions. Hiding data during transmission via Android apps emerged as an effective safeguard [2]. The primary motives behind choosing the subject of our study are to meet the demand for safe and convenient cardless transactions, enhance QR code security through advanced encryption to protect financial data, enhance digital payments, and reduce dependence on physical cards, offering an innovative solution that can serve as a model for researchers and developers. The proposed research strives to create a robust mobile app for secure cardless transactions, assess its performance and effectiveness, compare it to existing systems, provide practical recommendations, and ultimately contribute to the advancement of mobile security technology in financial transactions. The scope of our proposed approach includes creating a secure mobile application for cardless transactions by integrating QR code authentication with a hybrid algorithm consisting of AES and ECC algorithms. This study focuses on technical implementation, excluding economic or social aspects. We expect our proposed approach to create a secure mobile application for cardless transactions. Evaluate the feasibility of QR code authentication and cryptographic algorithms in mobile transactions and identify and resolve security vulnerabilities in existing mobile transaction systems. Given the paramount importance of security and authentication in mobile banking, our literature review explores

insights and fundamental research related to data encryption, authentication protocols, and transaction applications, all in line with the scope of our proposed research. Numerous mobile applications facilitate digital transactions, enabling users to conveniently perform bill payments and transfer funds globally through uncomplicated procedures using smartphones. The paramount significance lies in the security and authentication attributes of these applications, serving to safeguard user data and deter unauthorized access or misuse.

of sensitive information. The ensuing research endeavors furnish foundational insights into data encryption, authentication protocols, and transaction applications, aligning with the scope of the proposed research.

In the world of mobile banking, researchers have identified important features and functions that are available to users. Notably, [3] and [4] have discussed a variety of mobile banking features. These features include the ability to make bill payments, check account balances, send text messages, and easily scan and deposit checks using mobile devices, which can be done from different locations, including ATMs and banks. These features highlight the convenience and adaptability of mobile banking. Furthermore, users can efficiently send text messages through their mobile devices and find ATMs or banks without difficulty. These features indicate that users are satisfied with the convenience of banking services. Another advantage of mobile banking is its efficiency, which is demonstrated through straightforward operations such as secure withdrawals and easy account management, in line with the "anytime, anywhere" concept.

In her study on the role of perceived risk in user decision-making, [5] highlighted financial, performance, and privacy concerns. The utilization of mobile banking often instills apprehensions regarding potential financial loss attributed to connectivity issues or server malfunctions, significantly impacting both financial and performance aspects. Furthermore, privacy concerns escalate as online shopping applications amass personal information (e.g., name, address, phone), intensifying anxieties regarding data compromise. These identified risks detrimentally affect trust in mobile banking, presenting a challenge for its widespread adoption. Addressing this issue, [1] provided an insightful examination of mobile banking application functionalities, emphasizing security measures. Prominent applications like Tez/Google Pay, Paytm, PayPal, and Bhim integrate security features such as authentication, machine learning-driven fraud detection, transactional PINs and one-time passwords (OTPs), Transport Layer Security (TLS) connection, and secure user credentials. For a comparative overview of the security features across these applications, refer to Table 1.

TABLE 1. shows a comparison of the security features of the mentioned applications. [1]

Basis for comparison	Paytm	BHIM	Tez/Google pay
Auto logout feature	No	Yes/Timeout	Yes
Authentication	Username and password, Biometric authentication	Password (4- digit-UPI pin)	Google PIN or screen lock
Confidentiality	OTP	3-Factor Authentication.	Audio QR (QAR) and UPI Pin
Transaction time	Medium	High	Low
Cash Mode	No	No	Yes
Access without internet	Phone call and secured Paytm PIN	Unstructured Supplementary Service Data (USSD) based	USSD based

The study by [6] extensively explored the complexities associated with data security challenges, encompassing data protection methodologies and the spectrum of cyberattacks employed by malicious entities to infiltrate transactional systems. Utilizing symmetric encryption methods, notably the Advanced Encryption Standard (AES), in conjunction with asymmetric encryption techniques such as Elliptic Curve Cryptography (ECC), has proven highly effective in ensuring data confidentiality. The authors proposed a secure and optimized framework aimed at enhancing data-sharing paradigms within the cloud environment while prioritizing data security and integrity. This framework leverages the synergy between ECC and AES, amalgamating their capabilities to guarantee authentication and maintain data integrity. Rigorous experimental evaluations validated the efficiency of the proposed approach, demonstrating superior outcomes compared to existing methodologies. In a related study, [2] investigated symmetric and asymmetric algorithms, highlighting their relevance in cloud computing. Symmetric algorithms, exemplified by the 256-bit AES method, are favored for banking services due to their resource efficiency and faster processing. Conversely, asymmetric algorithms find utility in Android devices, addressing challenges posed by symmetric key lengths in mobile environments. Encryption emerges as a critical facet of transactional security, necessitating meticulous selection of encryption algorithms to ensure comprehensive information and data security. Assessment of encryption algorithms considers various criteria encompassing memory requirements, power consumption, encryption and decryption speeds, key generation and execution times, key size, and signature generation and verification times. The literature underscores the ECC algorithm as the latest, most efficient, and highly effective encryption method, particularly suited for Android applications and mobile devices. Comparative analysis between ECC and RSA reaffirms ECC's

superiority in terms of effectiveness and safety, as delineated in Table 2. Given these findings, the researchers strongly advocate for the adoption of the ECC algorithm, underscoring its superior security levels and expedited performance.

TABLE 2. Comparison between RSA and ECC [2]

Security	RSA	ECC
80	1024	160
112	2048	224
128	3072	156
256	15360	512

Nguyen Tran [7] extensively discussed the application of the elliptic curve algorithm as an asymmetric cryptographic framework in the development of a Smart-Auto Parking system. The study unequivocally demonstrated the superior efficacy of elliptic curve cryptography (ECC) compared to the widely adopted RSA algorithm. The presented system showcases enhanced security capabilities relative to existing market alternatives. Additionally, deploying the program on smartphones enhances user convenience while concurrently reducing capital expenditure. In a related study, Smith et al. [8] proposed a two-tier encryption model and a model aimed at enhancing data security within cloud computing. This model incorporates the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) to bolster data protection against unauthorized intrusion and third-party access. This integration yields comprehensive enhancements, ensuring data confidentiality, integrity, cryptographic efficiency, and user trust within the Cloud Computing (CC) environment. The adoption of ECC's smaller cryptographic keys significantly accelerates cryptographic processes, thereby augmenting the operational velocity of the platform. The research thoroughly analyzes cryptographic operation duration, and intrusion prevention mechanisms, and establishes user trust.

In light of the rising instances of fraud and identity theft, ensuring secure validation of user identification is paramount for online transactions. Digital authentication methods are increasingly prominent for enhancing user trust in identity verification; however, they remain susceptible to security breaches. Current research endeavors to address and mitigate the security inadequacies and challenges associated with digital authentication.

In a study by [9], a cardless transaction system was introduced employing one-time password (OTP) authentication, regarded as more secure than conventional password-based authentication. However, this system faces challenges related to data confidentiality and integrity during transactions due to inherent limitations. Addressing these concerns, [10] devised an OTP authentication method utilizing the one-time pad algorithm, generating ciphertext unrelated to plaintext and offering a high level of security. Despite the effectiveness of OTP, its use via SMS has been identified as susceptible to attacks. In response, [11] proposed the utilization of QR codes to transmit data via the bank's server, enhancing security as the decoding process is exclusively managed by the bank. Conversely, [12] suggested an alternate approach employing Near Field Communication (NFC), incorporating multi-factor authentication such as transaction details, facial recognition, a 4-digit personal identification number, and a smartphone with NFC capabilities. To counter ongoing malware threats, which present a persistent risk to system security, [13] presented a comprehensive five-phase authentication scheme encompassing User ID, User password, Unique user ID, matching the user's QR code and password with the UID, all fortified through the application of RSA and MD5 algorithms. Augmenting authentication by associating QR codes with unique identifiers contributes to enhanced security measures. In addressing challenges presented by cybercriminal activities, [5] proposed a solution involving the encryption of transactional information. This strategy restricts data access solely to individuals possessing the corresponding private key. The proposed approach integrates the Elliptic Curve Cryptography (ECC) asymmetric algorithm with Quick Response (QR) codes. The procedure involves the mutual sharing of public keys between the financial institution and the customer. Subsequently, transaction data is encrypted using both the public and private keys. The encrypted data details are encapsulated within a QR code, which the customer can scan using an Android application, enabling the retrieval and display of decrypted data.

This paper is structured as follows: In Section 2, the techniques used are described, and the requirements and design specifications are specified in Section 3, In Section 4 architecture of the proposed system. Executing Sections 5 and 6, the evaluation methodology that will be used to test the strategy and make improvements is explained. Finally, a discussion of the conclusion and future efforts

II. RESEARCH METHODOLOGY

Drawing upon insights from prior research, it is clear that integrating authentication and data encryption is crucial in transaction systems to guarantee security. In light of this, we have devised an innovative methodology to bolster the security of current transactions. The proposed system integrates both mutual authentication and data encryption, employing an advanced encryption

algorithm in conjunction with an asymmetric elliptic curve fusion technique. To uphold data privacy and permanence, we employ QR codes for data masking and secure storage on mobile devices.

Proposed Methodology

Our proposed approach encompasses three key stages:

1) Installation and Registration:
   a. Users install a secure application provided by the banking institution, incorporating essential information and data.
   b. Authentication is achieved by inputting the institution-provided password and email address during login.
   c. Successful registration grants users access to the secure application and its functionalities.
2) Encryption and Secure Data Transmission:
   a. Users initiate the data exchange process with another user.
   b. Transaction specifics, including the recipient's account number, are entered.
   c. Employing a hybrid algorithm with embedded encryption keys, the data is encrypted.
   d. A QR code is generated to securely store the encrypted data, and is saved on the user's mobile.
   e. To transmit the data to the recipient, an image of the QR code is sent via email, requiring an additional authentication password.
3) Reception and Decoding:
   a. Upon data reception, the recipient is notified and provided a QR code.
   b. The QR code is saved on the recipient's device.
   c. The recipient scans the QR code, by Utilizing the secure application on their mobile phone.
   d. The decryption key within the hybrid algorithm is utilized by the recipient to decrypt the data securely.
   e. Finally, the data will be decrypted and displayed securely.

III. DESIGN SPECIFICATIONS

Current research introduces an Android application facilitating user registration and program utilization. The design of the proposed method delineates a systematic and detailed procedure, focusing on securing data transmission and fostering effective user communication. The Android application's design is elucidated using a flowchart and system architecture, offering a comprehensive depiction of the envisaged system.

System Architecture

The functional operation of the system is illustrated in Fig. 1. The system is composed of users, banking institutions, and Firebase servers, interconnected through a central Firebase server dedicated to messaging and data exchange functionality.

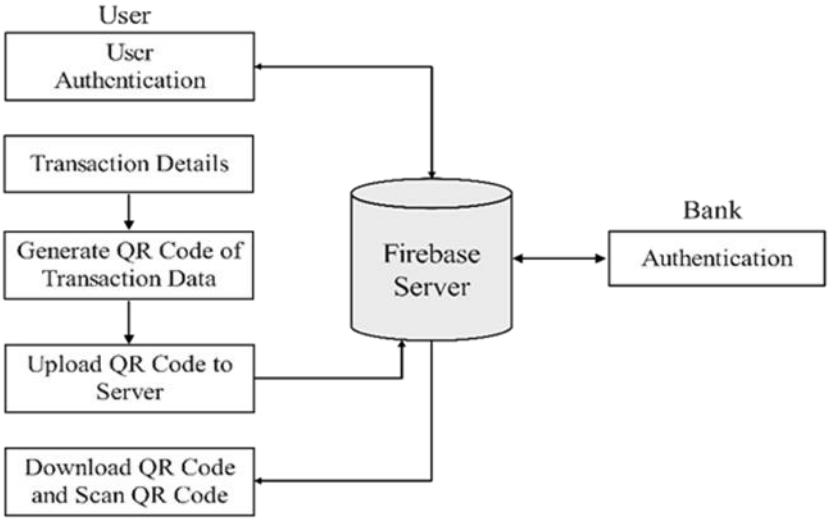


Fig. 1. Architecture diagram System

Proposed Framework

In this section, we present an elaborate exposition of the suggested framework, underscoring the pivotal role of amalgamated technology involving the Elliptic curve Code (ECC) and Advanced Encryption Standard (AES). Additionally, we emphasize the incorporation of Quick Response (QR) codes to bolster security during the transmission of data.

Mobile Application

The mobile application serves as the interface through which users engage with the system. It is responsible for generating and presenting the QR code, receiving encrypted data from the QR code, decrypting it utilizing the hybrid AES/ECC algorithm, and displaying the decrypted information to the user.

QR Code Generation

The QR code generator is tasked with creating the QR code containing encrypted data. This process employs Hybrid ECC-AES technology to encrypt the data before embedding it into the QR code.

Firebase

Firebase represents a comprehensive platform offering diverse services for mobile applications, including authentication, message exchange, database management, and storage functionalities. Mobile app developers can leverage these services to construct robust and dependable applications capable of managing user authentication, data storage, and communication with fellow users.

Hybrid ECC-AES Algorithm

- Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography (ECC) stands as an efficient encryption technique employing elliptic curves over finite fields, known for its security, computational efficiency, and utilization of short keys. Particularly suited for resource-constrained mobile devices, ECC surpasses RSA in performance, ensuring secure data handling on such devices.
The Elliptic Curve Cryptosystem (ECC) leverages the mathematical properties of elliptic curves to enable the use of short keys. Key generation involves both private and public keys. ECC's security is founded on the curve equation:

$$E = \{(X,Y) : Y^2 = X^3 + aX + b \pmod P\} \quad (1)$$

The private key (d) gives rise to a public key (Q) through scalar multiplication with a generator point (G):

$$Q = d\,G\ [14] \quad (2)$$

- The Advanced Encryption Standard (AES):

AES, a symmetric block cipher, employs a single key for both encryption and decryption. Data is segmented into fixed blocks, and AES operates in versions of AES-128, AES-192, or AES-256, distinguished by the number of rounds. NIST officially sanctioned AES in 2001 [15], acknowledging its merits in security, efficiency, and encryption of cloud data. Contemporary studies reaffirm that AES is memory-efficient, robust, and expeditious in both encryption and decryption processes, rendering it well-suited for speed-sensitive applications.

- AES Encryption and Decryption Procedure:

1) Encryption:
   a. Byte Substitution: Data is substituted using an S-box, resulting in a 4x4 matrix.
   b. Shift Rows: Shifting of rows to the left by 1, 2, and 3 bytes, respectively.
   c. Mix Columns: Application of a specific mathematical function for column mixing.
   d. Add Round Key: State is XORed with a segment of the encryption key.

2) Decryption:
   a. Add Round Key: The inverse function is applied using keys in reverse order.
   b. Inverse Shift Row: Rows are shifted to the right by 1, 2, and 3 bytes.
   c. Inverse Byte Substitution: Inverse S-box is employed for substitution.
   d. Inverse Mix Column: Reversion of mix columns through GF (28) polynomials.

ISSN: 2710-2165

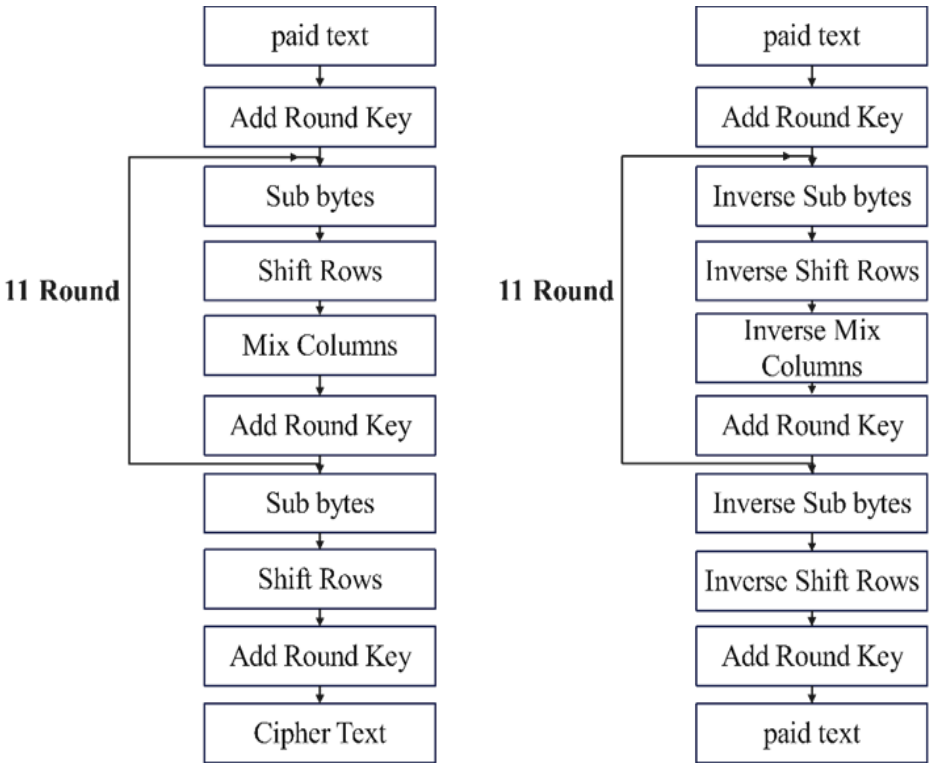


Fig. 2. Encryption / Decryption AES [6]

- Hybrid ECC-AES Algorithm:

Although Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) are extensively employed and offer substantial advantages, they are not immune to vulnerabilities. The effectiveness of AES encryption is intricately tied to the strength of the encryption key used. Weak or compromised keys can compromise the security of the encrypted data, underscoring a limitation of AES. On the other hand, ECC introduces an issue of increased encrypted data volume and complexity, which can elevate the risk of errors during computation, thereby diminishing overall security.

Previous research indicates that the standalone AES encryption method is marginally slower compared to the hybrid ECC-AES approach, primarily due to AES employing a larger key size. In contrast, the hybrid approach capitalizes on a smaller key size, enhancing speed and robustness in data security. Leveraging ECC in conjunction with AES results in a reduced key size and improved performance, aligning with ECC's characteristic of a smaller key size. ECC establishes standards for encryption and decryption keys, effectively reducing the key size and enhancing the security of the system. The integration of ECC with AES represents an optimal approach for data protection, offering a safeguard against unauthorized access.

- Proposed Approach for Hybrid AES/ECC Implementation:

Upon input of the text, it undergoes encryption using AES, employing a key generated through ECC. Subsequently, the recipient decrypts the data utilizing this key, retrieving the original plain text. The depicted figure visually elucidates the encryption and decryption processes involving AES-ECC operations, as illustrated in Figure 3.

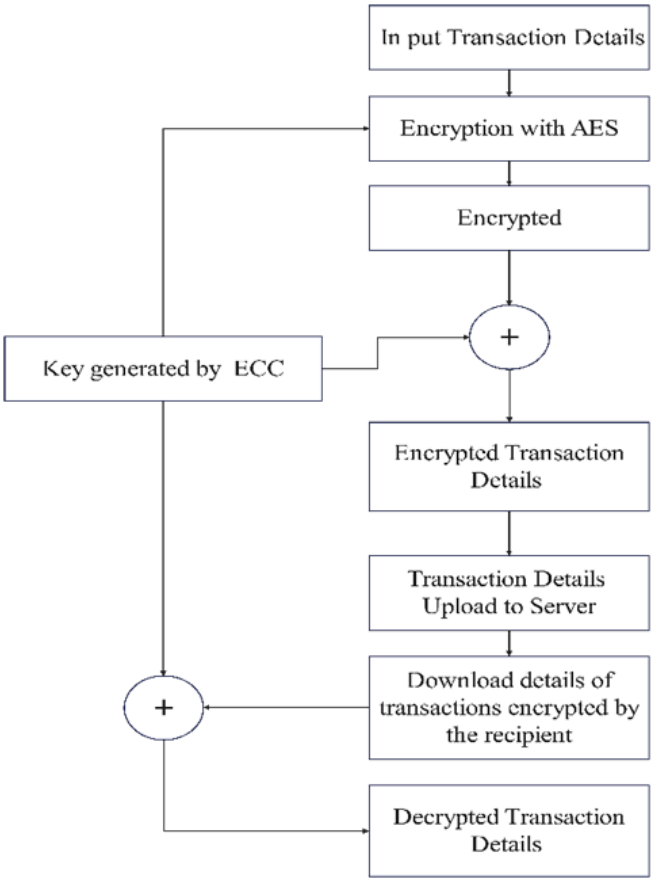


Fig. 3. AES-ECC encryption and decryption operations [16]

- Benefits of the Hybrid Algorithm:

Research has demonstrated that amalgamating AES and ECC algorithms in a hybrid presents a compelling strategy to augment the security and efficiency of cryptographic systems. This integration leads to a reduction in key lengths, facilitating proficient encryption and digital signature procedures while upholding ciphertext confidentiality. Moreover, the hybrid algorithm allows for efficient recovery of original information from encrypted data using the decryption key.

IV. ARCHITECTURE OF THE PROPOSED SYSTEM

1) To commence system utilization, the user is required to create an account within the application using their designated email ID and bank-specified password.
2) Upon successful account creation, Firebase generates a distinct User ID for each user on the server end, managing and monitoring user actions through this identifier.
3) Upon logging in, transactions designated for exchange are encrypted using the AES algorithm and the ECC-generated public key.
4) Subsequently, an encrypted data QR code is generated for transaction encapsulation.
5) The QR code, containing the encrypted data, is then transmitted to the intended recipient via email.
6) The recipient preserves the QR code on their mobile device.
7) The recipient adheres to registration procedures and proceeds to log in. The recipient scans the QR code and decrypts it utilizing the same ECC-generated public key.

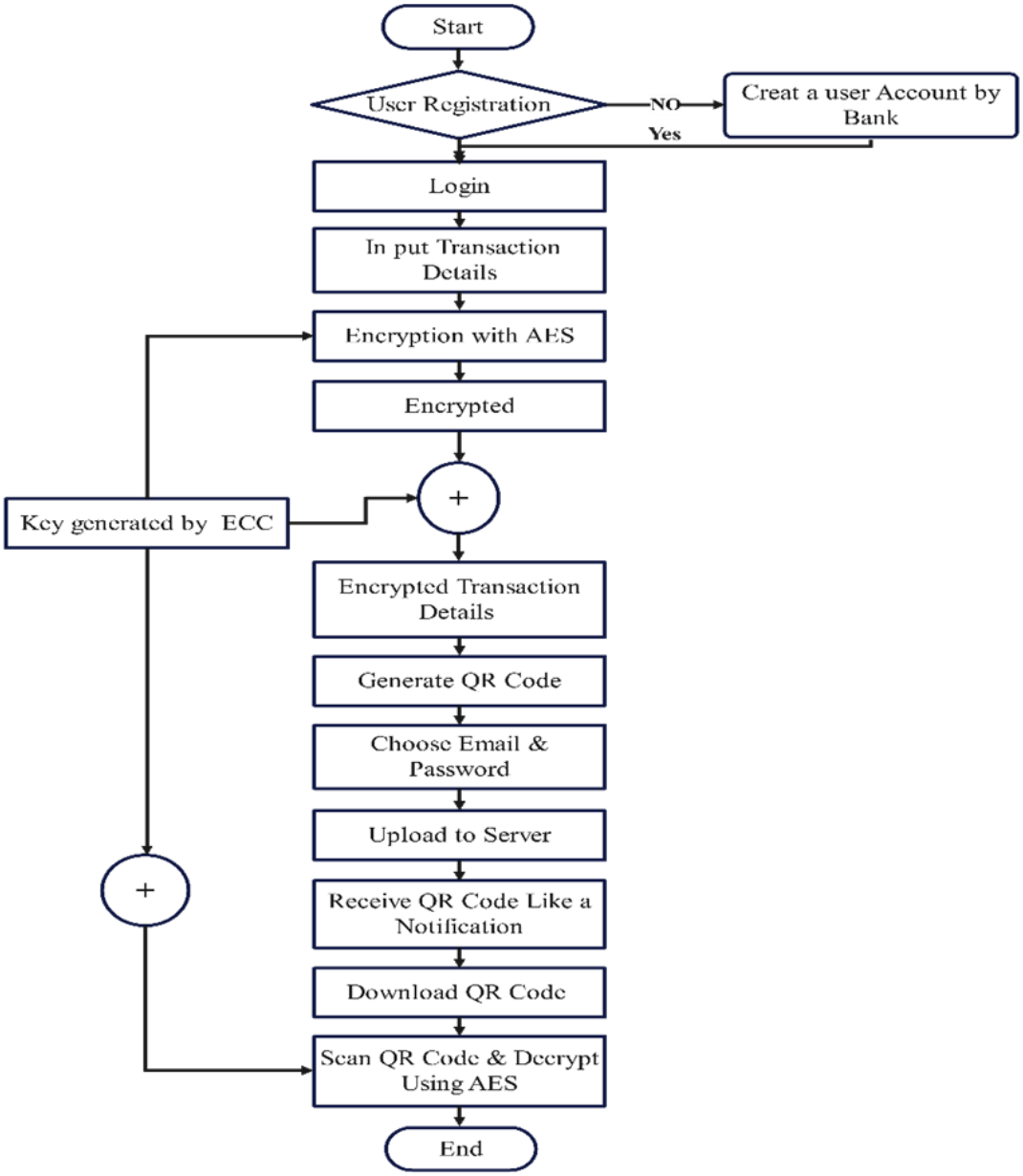


Fig. 4. Flow diagram of the application

V. IMPLEMENTATION

The proposed system is enacted via the development of an Android application. This section delineates the procedural steps involved in constructing the application from its inception.

Cryptographic Standards and Specifications

To uphold cryptographic security within an Android application, the Android platform is endowed with intrinsic security features that facilitate data compartmentalization, encryption, and data safeguarding through cryptographic mechanisms. Integration of a hybrid cipher system amalgamating ECC-AES is achieved through the utilization of the Pointy Castle library. This library offers the practical realization of both symmetric and asymmetric encryption, hashing, digital signatures, and diverse cryptographic functionalities, encompassing the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Integrated Encryption System (ECIES). In our proposed system, we have adopted the AES-128 encryption standard employing a 128-bit key size. Moreover, we have instantiated the ECDSA encryption standard for elliptic curve cryptography, employing a key size of 256 bits.

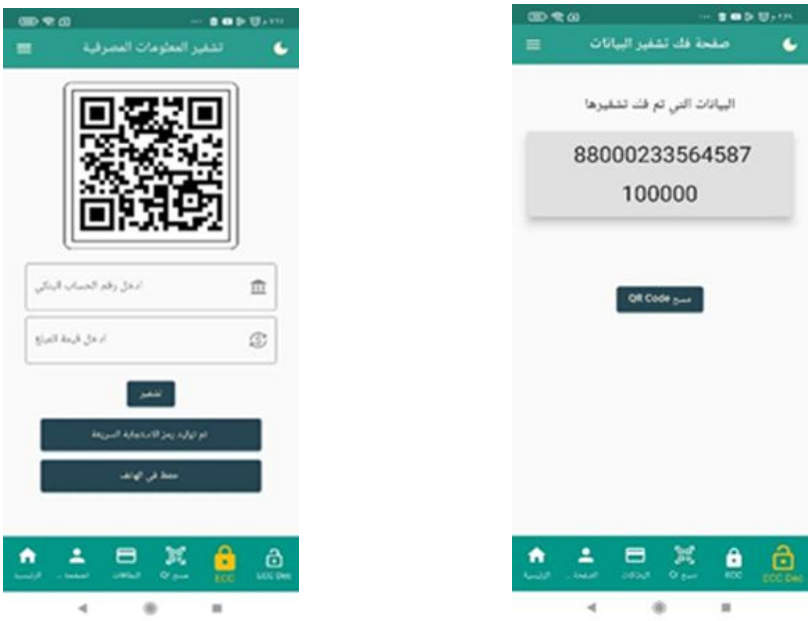
Server Deployment

This application utilizes Firebase services for user authentication (Auth), cloud messaging, and real-time database management. Firebase offers a comprehensive platform for mobile and web application development, replete with requisite tools and services. Application creators are mandated to establish an account with Firebase and seamlessly integrate their applications with Firebase services. The Android Studio IDE must incorporate a Firebase plugin and be linked to Firebase through a developer account. User authentication with the application is facilitated through the email and password method. The authentication service generates a unique customer ID for utilization across various functional aspects. Firebase also furnishes a real-time database, typically employed for storing QR code images. However, our proposed system adopts a mobile-based QR code storage approach. QR code images are stored locally on the mobile device and are dynamically retrieved for scanning purposes within the application.

Development of an Android Application

The Android application was constructed using the Flutter framework and the Dart programming language to create the graphical user interface (GUI) within Android Activity classes. The design of the GUI was achieved through XML layouts. Firebase was employed to facilitate data transmission and QR code storage through a real-time database. This section provides a detailed examination of the functionality and performance of the proposed system, outlining procedural steps. The initial phase involves installing the secure application on the user's mobile device, followed by user registration. User data is securely stored on the server and utilized for authentication purposes. The user-centric application offers features such as password recovery and registration options. Additionally, to enhance security, the system enforces an automatic logout when switching to another application on the mobile phone, such as WhatsApp or making a phone call.

Enhanced Security Measures Incorporated within the application is a security protocol wherein if the login process exceeds a predetermined duration of five seconds, the application will autonomously terminate, thus fortifying the data against potential intruders. Following a successful login and transaction initiation, the user can solicit the account number from another user through email or other preferred communication channels. Subsequently, the sensitive data undergoes encryption utilizing a hybrid algorithm technology, The QR code is then generated. To heighten the security of transmitted transactions, the recipient's email necessitates an additional password for authentication. The QR code, representing the encrypted data, is then generated and stored on the mobile device, as depicted in Fig. 5, (a). Upon scanning the QR code, the embedded key derived from the hybrid algorithm, generated earlier through the ECC algorithm, is employed to decrypt the data, as illustrated in Fig. 5, (b).



(a) (b)

Fig. 5. (a) Encryption and QR Code Generation, (b) Decryption and QR Code Scanning

VI. EVALUATION OF THE PROPOSED APPROACH

The efficacy of the proposed approach was assessed by scrutinizing its security attributes through a comprehensive checklist and assessing the efficiency of its cryptographic functions by measuring the computational time for logical output determination. Furthermore, a comparative analysis was conducted to gauge the robustness of the system against prior efforts within the domain.

Security Enhancements

1) Preceding transmission, data underwent encryption to ensure its confidentiality.
2) The encrypted data was encoded into a QR Code to conceal its contents.
3) A robust encryption mechanism employing keys within a hybrid algorithm (ECC-AES) was utilized, ensuring comprehensive data protection inaccessible to users.
4) Data integrity was preserved by securing data using the QR code, impervious to server access.
5) Multi-factor authentication was employed to bolster transactional security.
6) Integration of an auto-logout function activated after a predefined idle period or in the event of the user's phone loss.
7) Automatic logout functionality was implemented upon the user's interaction with other applications such as WhatsApp or making phone calls.

Performance Evaluation of Security Functions

Numerous operations were executed during application runs to quantify the computational time of cryptographic functions. The outcomes are delineated in Table 3.

TABLE 3. Elapsed Duration of the Functions

Function	Test Run 1 (ms)	Test Run 2 (ms)	Test Run 3 (ms)	Average (ms)
Encryption	76	79	81	78.66
QR Code Generation	0.02	0.02	1	0.34
QR Code Scanning & Decryption	26	23	24	24.33

The obtained results demonstrate a high degree of consistency, as evidenced by the satisfactory duration observed for encoding and decoding, as well as the swift execution of QR code creation and scanning functions. These quantifiable measures are contingent upon numerous factors, encompassing hardware architecture specifications, network connectivity speed, and the inherent intricacy of both encrypted and unencrypted data sets.

Comparison with Prior Research

A comparative analysis was conducted between the proposed innovative system and the study by [5], as outlined in the referenced academic publication titled "Secure Cardless Transaction Android Application using ECC Algorithm and QR Code".

Secure data Cardless using a Mobile App by Combining QR Code with a Hybridization of AES and ECC Algorithms	**Secure Cardless Transaction Android Application using ECC Algorithm and QR Code [5]**
A hybrid Algorithm (ECC-AES) was used.	ECC Algorithm only.
Encoding Time: ECC-AES (78.66).	Encoding time: ECC Algorithm (47.33).
Decoding Time: ECC-AES (24.33).	Decoding time: ECC Algorithm (10.33).
Encryption Mechanism: Public key with AES.	Encryption Mechanism: Public key (encryption) and Private key (decryption)
Key Handling: Embedded and secured within a hybrid algorithm (inaccessible to users).	Public-private key usage by individual users Server
QR Code Storage: Mobile device.	QR Code Storage: in the server.
Authentication: Multiple authentications.	Authentication: Single authentication.

Comparing the proposed application with the previous application revealed an enhanced level of security, albeit at the expense of longer encryption and decryption durations due to the use of both symmetric and asymmetric encryption approaches. The integration of symmetric AES and asymmetric ECC algorithms, known for their compatibility, leads to robust encryption and heightened security.

The practice of embedding keys within the algorithm augments security, rendering data less accessible to unauthorized individuals. This approach not only fortifies the system against potential attacks but also streamlines key management processes, contributing to overall system efficiency.

VII. LIMITATIONS OF THE PROPOSED RESEARCH

The primary scope of the proposed system centers on ensuring secure data transmission and authentication. Particular emphasis is placed on safeguarding transaction data by implementing measures for privacy and data consistency.

VIII. DISCUSSION

To evaluate the alignment of the proposed system with its intended objectives, a comprehensive evaluation encompassing essential factors was conducted. A comparative analysis was performed against preceding solutions to ascertain the system's superior efficacy in addressing existing challenges. The evaluation encompassed both performance and security assessments. The primary objectives of the application were twofold. The first objective was to ensure secure transactions within a server infrastructure, concurrently establishing a robust authentication mechanism. This was effectively accomplished using a mobile app by integrating a QR code and hybridizing AES and ECC algorithms. Empirical feedback from this assessment affirms the successful attainment of predetermined objectives.

IX. CONCLUSION

The principal aim of this study was to develop a secure Android banking application enabling safe data transmission and authentication, mitigating ATM card theft and unauthorized access to cardless banking applications. An extensive literature review revealed various technologies addressing secure data transfer and authentication; however, our proposed approach effectively fulfills current requirements for secure transactions. A notable advantage of our approach lies in the integration of encryption and decryption keys within the hybrid algorithm, fortifying the system and adding an extra layer of defense against potential attacks. To mitigate key embedding drawbacks, stringent measures were implemented to restrict application access. The storage of the QR code on the customer's mobile phone offers several advantages, facilitating easy and prompt access, even in offline or limited internet connectivity scenarios. Our approach excels in providing heightened security and faster performance by leveraging symmetric and asymmetric encryption methods through ECC-AES hybrid technology, surpassing applications utilizing ECC methods. Future endeavors may extend this approach to enhance authentication and secure transactions in online banking platforms and payment machines, potentially integrating additional layers of protection such as fingerprint or facial recognition (Multiple Authentication).

REFERENCES

[1] N. K. and B. Janet, "An analysis of the balance between security and utility of mobile applications," in *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India*, 2018, pp. 1-4, doi: 10.1109/ICCSDET.2018.8821080.

[2] F. Mallouli, A. Hellal, N. Sharief Saeed and F. Abdulraheem Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France*, 2019, pp. 173-176, doi: 10.1109/CSCloud/EdgeCom.2019.00022.

[3] J. Yu and C. Nuangjamnong, "The Impact of Mobile Banking Service on Customer Satisfaction: A Case Study of Commercial Banks in China," *United International Journal for Research & Technology*, vol. 3, no. 10, pp. 43-64, 2022.

[4] H. Lee, Y. Zhang, and K. L. Chen, "An exploration of attributes and security aspects in the context of mobile banking strategy," *Journal of International Technology and Information Management*, vol. 22, no. 4, pp. 2, 2013.

[5] B.S.Ponnsamudra *"Secure Cardless Transaction Android Application using ECC algorithm and QR code,"* M.S. thesis, National College of Ireland, Dublin, 2019.

[6] S. Rehman et al., "Hybrid AES-ECC model for the security of data over cloud storage," *Electronics*, vol. 10, no. 21, pp. 2673, 2021.

[7] N. T. T. Lam and L. T. Tra, "Elliptic Curve Cryptography (ECC) algorithm and its application in Smart-Auto Parking Systems," presented in *2021 IEEE Conference on Intelligent Transportation Systems*, 2021.

[8] H. D. K. Mawuli, D. R. Korda, and E. D. Ansong, "An enhancement of data security in cloud computing with an implementation of a two level cryptographic technique, using AES and ECC algorithm," *Electronics*, vol. 9, no. 9, pp. 639-650, 2020.

[9] M. A. Imran, M. F. Mridha and M. K. Nur, "OTP Based Cardless Transction using ATM,"in *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, Dhaka, Bangladesh, 2019, pp. 511-516, doi: 10.1109/ICREST.2019.8644248.

[10] S. Wahjuni and R. Pristian, "Android-based token authentication for securing the online transaction system," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), 2016, pp. 174-177, doi: 10.1109/ICTC.2016.7763462.

[11] D. Kumar, A. Agrawal and P. Goyal, "Efficiently improving the security of OTP," in *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, India, 2015, pp. 912-915, doi: 10.1109/ICACEA.2015.7164835.

[12] A. Adukkathayar, G. S. Krishnan and R. Chinchole, "Secure multifactor authentication payment system using NFC," in *2015 10th International Conference on Computer Science & Education (ICCSE)*, Cambridge, UK, 2015, pp. 349-354, doi: 10.1109/ICCSE.2015.7250269.

[13] N. Sharma and B. Bohra, "Enhancing online banking authentication using hybrid cryptographic method," in *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, India, 2017, pp. 1-8, doi: 10.1109/CIACT.2017.7977275.

[14] Y. Yuhan, "The Overview of Elliptic Curve Cryptography (ECC)," *Journal of Physics: Conference Series*. vol. 2386, no. 1, IOP Publishing, 2022.

[15] "National Institute of Standards and Technology, FIPS 197 - Advanced Encryption Standard (AES)," Computer Security Resource Center, [Online]. Available: https://csrc.nist.gov/pubs/fips/197/final. [Accessed: 24/10/2023].

[16] Sharma and V. Chopra, "Analysis of AES Encryption with ECC," in *2016 17th International Interdisciplinary Conference on Engineering Science & Management*, Dubai, UAE, 2016.