International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

A Secure Payment Method for Mobile Wallet Framework

Sunil Mankotia
Department of Computer Science, Himachal Pradesh University, Shimla, (HP), India
E-Mail ID : mankotia.sunil@gmail.com

Article Info
Volume 9, Issue 4
Page Number : 710-721

Publication Issue
July-August 2022

Article History
Accepted : 01 August 2022
Published : 16 August 2022

ABSTRACT

Mobile wallets are very convenient and helpful in the day-to-day transactions of money and it is of utmost importance to enhance their security levels. The present study develops a secure and convenient m-Commerce application and an electronic wallet for smartphones using the mobile wallet framework. The proposed method is for making financial transactions using Mobile Wallet, which includes adding money to the wallet, sending money to another person, making bill payments etc. The user selects the option from the wallet and the parameters related to the transaction are encrypted using the AES-256 algorithm and the same session key and cipher text is obtained. Parameters will depend on the type of transaction selected by the User. Thereafter, the cipher text obtained is forwarded to the cloud server and financial transaction is facilitated using the payment gateway integrated with the proposed application. The performance of the proposed methods has been compared with those of existing methods. After the analyses of various parameters, it has been shown that the performance of the proposed solution is much better as far as the efficiency of operations and security of transactions are concerned.

Keywords : Mobile Wallet, AES-256, Payment Gateway, Financial Transaction.

I. INTRODUCTION

In today's world, mobile devices and smartphones are being used extensively and as such, are essentially becoming the most sought-after requisites of an integral part of life. The development of several applications feasible for these devices has been creating a huge demand as well as scope for applications of mobile devices in even the day-to-day routine of individuals. The applications of mobile devices range from online social indulgence to sales to marketing to services to financials to e-governance to security and the list is endless. However, one significant issue related to the entire spectrum of such devices and their applications is the restrictions/ limitations on device capability as far as the resources like the power of the processor, consumption of energy and available memory are concerned. The technologies that provide some of the answers (or at least intend to) to these issues are mobile computing and cloud computing. Modern mobile architectures integrate both cloud computing as well as mobile technology to cater to most of such upcoming issues [1]. Cheung

and Newport in [2] have stated that mobile cloud computing is a new technique where most of the processing, data storage and computation accompanied by the applications can be moved either fully or partially, from the mobile devices to the centralized strong platforms of computing residing on the cloud. Mobile Cloud Computing was established after the cloud computing concept got established to a large extent. It has been attracting the attention of businessmen all over the globe as a profitable field that decreases the development and running costs of mobile users as well as mobile applications. This technology helps to a) accomplish richer experiences of different mobile services at reduced costs, and b) provide promising solutions to the applications covering the latest horizons using fundamentals of core information technology. Li in [3] has concluded that the capability to assess applications and data from anywhere and at any time with reduced cost is the most essential advantage of mobile cloud computing. But such mobile applications based on huge mobility models and third-party cloud environments entail quite a few security risks too. The main security problem with Mobile Cloud Computing is securing remote applications and data from illegal accesses. The authorized users of mobile cloud computing-based applications are generating, processing and storing huge data. Since the mammoth amounts of data being generated by these users on the net are conveniently stored on the cloud servers at very low costs, the ownership of this data does not rest with them, more so because mostly these authorized users are seamlessly using each other's data. The data stored on the cloud can also be accessed by the service providers or unauthorized users too. There is a strong possibility of unauthorized access to this data by third-party users known as hackers. This unauthorized access to the data can at times, be dangerous. Therefore the issue of security in mobile cloud computing has become one of the major areas of research.

Smartphones have got integrated into mobile cloud computing technology almost instantly. Smartphones and mobile cloud computing are supplementing each other. According to Chowdhury and De, smartphones are getting smarter and are offering different applications and services over a wireless network to bring the world in front of the owner of the mobile phone [4]. If a user needs to access the accurate fare for a transport system or make a payment with some discount without the involvement of MCC, the evaluations become time-consuming and complex. In such a scenario, the worst case can occur when someone loses a physical wallet. The wallets normally contain various cards like ATM cards, Debit cards, Credit Card, Aadhar Card, PAN Card etc. The loss of the wallet requires blocking the cards immediately and the intimation to the law enforcement agencies to prevent any misuse which further requires remembering which cards the physical wallet contained along with their unique card numbers and then blocking each one of these manually. It would further require requests for the issuance of fresh/duplicate cards. This issue can be resolved by replacing a physical wallet with a digital wallet linked to an existing device of mobile like a smartphone. So, most of the effort to retrieve related information can be taken care of automatically.

II. LITERATURE REVIEW

Intruders or hackers have become very innovative in the current scenarios emboldened by the fact that most of the time they either cannot be traced or even if they are traceable, the limitations of laws hamper the proceedings. These malicious users indulge in intercepting, fabricating and modifying the user's financial and/or private information using many innovative techniques. Chen et al. in [5] have concluded that the effects of such unauthorized access to sensitive data are devastating in the cases of mobile commerce but the issue can be resolved using the NFC technique. This technique is a

familiar strategy and it can be used with a session-based alternative algorithm of cryptography to offer security in transactions based on a) mobile phone to mobile phone or b) Mobile phone to the points of service of various establishments like shops, third parties, online websites etc.

The cryptographic SIM card plays an essential role in securing confidential data. This strategy makes money transactions through mobile devices secured, securing the transaction data against interception, MIM attack, fabrication and modification. Grunberger and Langer [6] have confirmed that Near Field Communication (NFC), a wireless communication technique, assists device-to-device interactions within short distances without any distortion or hacking of data. This technique can be used for the transaction of money over wireless handsets or with any point of service.

The Near Field Communication enabled smartphones are helpful for direct money transactions from device to device. This concept can be used in the case of a mobile wallet too. As concluded by Isaac and Camara in [7], several mobile payment systems have been developed to permit payments for goods and services from mobile devices using various types of payments namely digital coins, credit card payments and micropayments. The relationship between the payer and the payee is limited in most of these mobile payment systems and these systems do not permit communication among different parties also. Moreover, in such cases, the merchant can't link to the Internet which causes great inconveniences and sometimes maybe, cost too for using third-party infrastructure to implement other communication processes between the acquirer and merchant.

Gao et al. have defined mobile payment as a wireless e-payment mode of mCommerce to assist financial transactions at POS using mobile devices [8]. Mobile payment systems based on wireless communication and services can be used by merchants along with information providers and content vendors to support and access transactions of payments driven by wireless-based applications of commerce. The revolution of mobile wallets is almost out of the stages of infancy but the successful service providers of this facility are far from determined. According to Sherman [10], the growth in mobile payments is quite impressive. Mobile payments have grown by over $1.3 trillion worldwide during the year 2017. More recently, the ability to purchase other goods and services through a mobile device has been a driver in the growth of many telecommunications establishments as a bill payment vehicle for mobile payments. Das and Samdaria in [10] have shown that presently when shopping in a wireless surrounding for instance to purchase something using SSL (Secure Socket Layer), one would have to send the expiry date, card number and other data to the merchant. The secure socket layer can assure the safety of peer-to-peer delivery but it cannot ensure the safety of underlying users' identities. To solve this issue the card network firms like Master-Card and Visa have put forward an e-payment specification of the system for Secure Electronic Transaction (SET). SET too struggles with its issues for instance a customer is required to apply for a certificate meaning thereby that on the side of the user, the corresponding data of the credit card must be stored in a hard disk. Shedid and Kouta in [11] have suggested that to improve the level of security, SET takes a long time to evaluate complex asymmetric decryption and encryption keys thus leaving users with an inconvenient experience of mobile commerce.

Nowadays, the compelling needs for mobile commerce are encouraging the players in the field to build a convenient and safe mechanism of mobile commerce [12]. Kadhiwal and Zulfiquar [13] predicted that mobile communication would continue to improve/develop new techniques and thus continue to provide attractive business opportunities. The solutions offered by the various vendors of mobile wallets should include innovative strategies to assist highly sophisticated client

applications in mCommerce through mobile devices to provide users with a highly simplified, user-friendly and safe environment. Similarly, the designers must continuously adapt existing mobile payment systems to permit clients to take benefit of the advantages related to the developing techniques while assuring reliable and secure transactions of payment. Patel et al. in [14] have suggested that a mobile wallet is an e-account which stores a customer's virtual money from which she/he can make a transaction using 3G/SMS/GPRS options. No bank account is involved in this concept as such. These techniques are trending in the revolution in the digital payment sector and are based on proximity techniques. The mobile wallets based on master-card servers are using secure e-transaction techniques and are being implemented to enhance the capabilities of secure transactions. Hence this kind of payment is used in dynamic surroundings to make the transaction between the vendor and the customer successful. The mobile wallet can link a mobile device to a vast number of cards and essentially other instruments of payment. Swarnalatha et al. in [15] have stated that the services of mobile wallets involved authentication of the user alongside other extra functions such as vending, transit, loyalty and ATM services. The integration of these functionalities is based upon the bricks-and-mortar concept of providing a cluster of mobile financial services extensive enough to fulfil the day-to-day requirements of a customer. Mobile device holders can make offline and online payments using electronic banking services, add electronic money to a local wallet or electronic purse, redeem electronic money, verify balances of payment accounts, use features based on location and view transaction histories using the mobile wallet. The mobile wallets also have the provisions to initiate disintermediation of payment [16]. The payment transaction processing initiated from these mobile wallets takes place outside of the traditional systems of card payment. They use the systems operated by non-financial institutions that may fall outside of the regulations and jurisdiction of the concerned authority. Thus mobile wallets may allow the usage of instruments of payment issued by both unregulated and regulated institutions, thus creating an interesting case for the rivalry between non-banks and banks in the retail payment sector. Joshi in [17] studied financial inclusion through mobile wallets with reference to India and stated that financial inclusion can be considered a very critical mechanism to attain rapid and constant growth. In India, 72% of inhabitants have a mobile phone. Moreover, with the introduction of mobile wallets, it has become exceptionally convenient for a person to make cashless dealings even without smartphones. The mobile wallet is proving especially effective in developing nations where desktop access to the internet and banking opportunities are still a privilege, yet mobile accessibility is extremely high. Joshi further concluded that the adoption of mobile wallets in India is growing at a very rapid pace and can certainly accelerate the process of financial inclusion along with traditional approaches to financial inclusion. According to Yadav, the rapid rise in the growth of mobile technology throughout the world has benefitted both customers and service providers [18]. For customers among a population that is underserved by traditional banking services, it is an opportunity for financial inclusion. On the other hand, for service providers, it opens up possibilities for financial institutions to deliver a great diversity of services at low cost to a large customer base of the poorest sections of society and people living in remote areas. The author of this study conducted a study to identify the active factors that influence people's intention to use a mobile wallet in India. Further, the study exhibited that its perceived usefulness of it positively influence the intention of potential customers to use/adopt mobile wallet. The model classified 96.5% of people in the category of adopting mobile wallet services whereas 35.4% of people for not have the intention to adopt/use them in future.

The mobile payment systems, due to the vagaries present in existing systems will continue to attract the attention of various academicians and industries. At the same time, security will be a major issue in mobile wallets. Thus it can be inferred that the adoption and deployment of different emerging techniques would bring new opportunities and barriers to the implementation and design of secure mobile payment systems nowadays and in future.

III. PROPOSED PAYMENT METHOD

The present work develops a smartphone-based application which can be used for financial transactions securely and conveniently. A payment method is proposed for making financial transactions using Mobile Wallet, which includes adding money to the wallet, sending money to another person, making bill payments etc. The user selects the option from the wallet and the parameters related to the transaction are encrypted using the AES-256 algorithm and the same session key and cipher text are obtained. Parameters will depend on the type of transaction selected by the User. Thereafter, the cipher text obtained is forwarded to the cloud server and financial transaction is facilitated using the payment gateway integrated with the proposed application. The proposed Key Server and AES-256 cryptographic processes are implemented using JAVA. The mobile wallet application is designed using Android OS. To evaluate the performance of the proposed model two types of evaluation have been carried out: a) measuring four parameters of time during the cryptographic process and b) measuring encryption time and data retrieval time for different file sizes under four settings. For the sake of evaluating the comparative performance of the proposed model, these measurements were compared with those of the existing models.

The steps involved in financial transactions supported by the proposed Mobile Application are shown in Figure 1.

The steps involved in financial transactions supported by the proposed Mobile Application are shown in Figure 1.

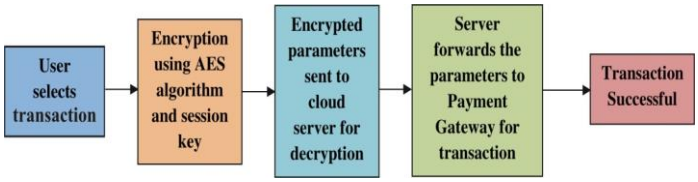

Figure 1: Secure Transaction

The secure transaction process consists of five steps the selection of a type of transaction by the user, encryption at the user end using AES algorithm and session key, encrypted parameters sent to the server, the Cloud Server forwards the desired transaction parameters to the payment gateway for execution, and it finally results in a successful and secure transaction. Each time when the user selects the option to send money to another user, receives the money or adds money from bank to wallet, the transaction parameters like amount, phone number, address, account number of sender or receiver, e-mail address etc. will be encrypted at user end using AES algorithm such that each transaction in the cloud becomes safe, and tampering of Uniform Resource Locator (URL) parameters could be prevented.

Proposed Secure Payment Transaction

Flowchart:

Figure 2 represents the flowchart that mentions the process flow of the secure payment transaction process executed.

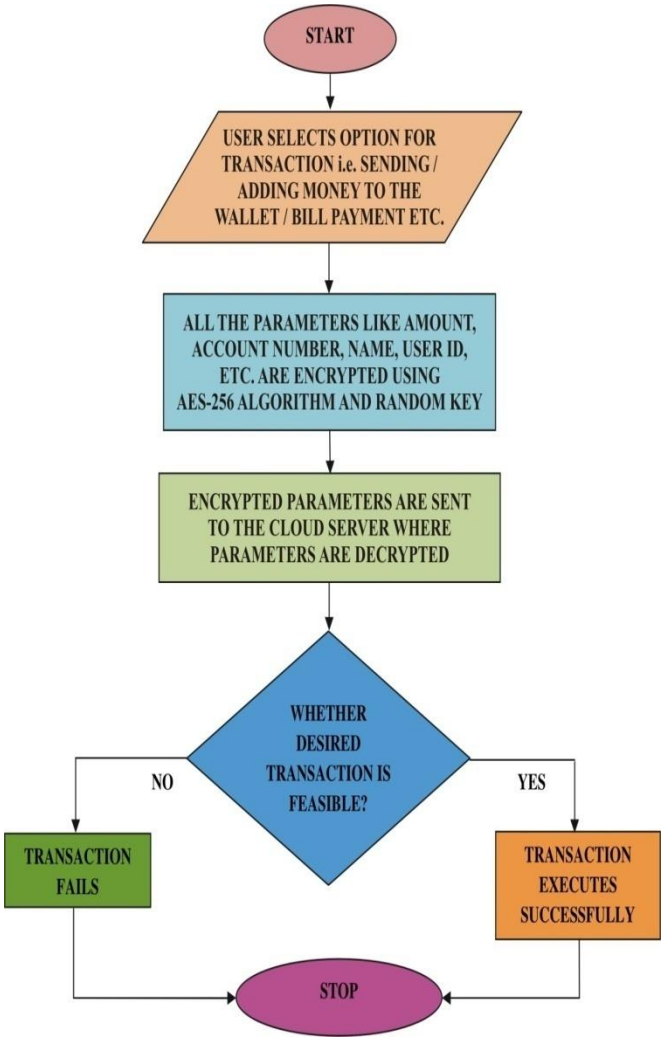

Figure 2: Flowchart Showing the Steps during a Secure Payment Transaction Process

To achieve a secure payment transaction, the following process should be done. In a secure payment transaction, the user selects the option as per his choice for sending, receiving or adding money to the wallet. The user data is required for this process to be executed. The different parameters are essential such as amount, account number, name, user id, e-mail, etc. These parameters are encrypted using the AES-256 algorithm. These encrypted parameters will be sent to the cloud server, and then the cloud decrypts it using the same AES algorithm and key. The cloud checks for the feasibility of the desired transaction. If it is feasible in terms of the available wallet amount, account number etc. then the transaction executes successfully; otherwise, it declines.

Secure Payment Transaction Algorithm

This algorithm is designed to enable users to make secure financial transactions. Users can select the desired option using the user interface of the proposed mobile application. As per the selection of the user, necessary fields are encrypted using *Enc2(), Enc3() or Enc4()* at the user end and forwarded to the cloud server for making the validation and necessary update in the database. If at any stage validation fails, an appropriate message will be displayed, and the transaction will not be accomplished; otherwise, the selected transaction will take place with the help of a payment gateway.

Algorithm 1. Secure Payment Transaction

1. **procedure:** SECURE_TRANSACTION

   Input: *transacttype, amt, ac_no, mobnum, name, bankname, ifsc*

   Output: TRUE if transaction successful; else FALSE.

2. **if**(transactiontype==1)
3. Obtain *accountno, mobnum, amt, name, bankname, ifsc*
4. **If** (*amt<=bal_amt*)
5. *Enc2()* the parameters with the **AES256** using the session key *k*
6. Use the PayUMoney sdk test app for transaction
7. Update *bal_amt*
8. **else**
9. transaction declines "Insufficient amount in your wallet."
10. **else if** (transactiontype==2)
11. obtain *mobnum, amt, mode*

12. *Enc3()* the parameters with the **AES256** using the session key *k*
13. Use the PayUMoney sdk test app for transaction
14. Update *bal_amt*
15. **else if** (tansactiontype==3)
16. obtain *clientID, amt, acc_no*
17. **If** (*amt<=bal_amt*)
18. *Enc4()* the parameters with the **AES256** using the session key *k*
19. Use the PayUMoney sdk test app for transaction
20. Update *bal_amt*
21. **else**
22. transaction declines "Insufficient amount in your wallet."
23. **end if**

Experimental Setup for Proposed Payment Method:

The experimentation and evaluation of the proposed design are validated using the Java platform. As of the year 2016, Java is one of the most widely accepted programming languages in use, particularly for client-server web applications with a reported 9 million developers. Java could decrease the costs, impel innovation, and advance application services as the programming language of option for IoT (Internet of Things), enterprise architecture, and cloud computing.

Android-based Mobile Payment Application is developed, and Cloud Server is implemented through Java. A Key Server is deployed in the same cloud for a generation of a random key for encryption and decryption purposes. Every time the user is provided with a unique session key for starting a session and performing transactions. A random key generation method is deployed for Key Server. AES algorithm with 256 bits of key length is used for encryption and decryption purposes. The exchange of information between these three entities is done through socket communication.

The payment gateway is integrated with the proposed mobile wallet to facilitate payment among different financial organizations or banks. The outcome of the proposed method executed in Java decides the superiority of the present research work.

IV. PERFORMANCE EVALUATION

Parameters Selected for Evaluation

There are specific performances to be evaluated to conclude the efficiency of the proposed research method. They are given as follows.

Key Generation Time

Key generation time is the amount of time taken to generate the key to encrypt and decrypt the user credentials such as username and password.

Encryption Time

Encryption time is the time taken to implement the encryption process. It is the total time taken to perform all the steps mentioned in the AES-256 encryption scheme.

Decryption Time

Decryption time is the amount of time required for retrieving the original information from the encrypted parameters.

Computation Time

The overall computation time required to complete a financial transaction using the proposed method.

Security Analysis

Security analysis is desired for advanced and extended technologies, concepts and methods which provide a secure server that leads to secure cloud computing. Security analysis of different existing schemes and the proposed scheme was made on specific parameters like confidentiality, the integrity of data, non-repudiation, efficiency, security against attacks, and convenience.

V. RESULTS WITH COMPARISON

The implemented model was executed and four parameters namely, key generation time, encryption time, decryption time and total time taken for execution were measured. The results so obtained were compared with existing methods.

Key Generation Time

The key generation time for the existing method and the proposed method is given below in Table 1.

Table 1: Key Generation Time for the Existing and Proposed Schemes

Key Generation Time (in ms)	
Existing Algorithm	**Proposed Algorithm**
6.5	4.2

Figure 3 shows that the key generation time for the existing method is 6.5 ms, and that of the proposed method is reduced to 4.2 ms. It is an improvement of approximately 35 per cent over the key generation time of the existing scheme. Again this is a significant improvement over the existing scheme.

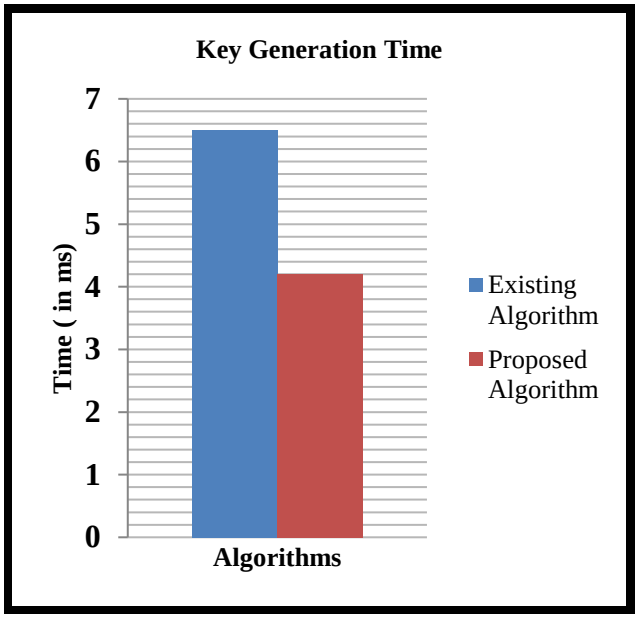

Figure 3: Comparison of Key Generation Time of Existing and Proposed Models

Encryption Time

The encryption time for the existing scheme and the proposed scheme is compared, and the values obtained are produced in Table 2 given below.

Table 2: Encryption Time for the Existing and Proposed Schemes

Encryption Time (in ms)	
Existing Scheme	**Proposed Scheme**
10.2	8.2

The encryption time required for the existing method is 10.2 ms. The encryption time required for the proposed method is reduced to 8.2 ms. It shows that there is an improvement of approximately 20 per cent in the encryption time of the proposed model in comparison to the existing model. The comparison of the result obtained in the form of a graph is shown below in figure 4.

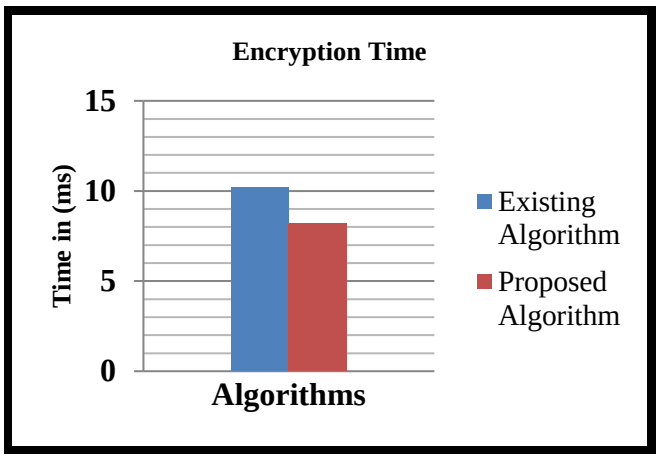

Figure 4: Comparison of Encryption Time of Existing and Proposed Models

Decryption Time

The decryption time required for the existing method and the proposed method is given below in Table 3.

Table 3: Decryption Time for the Existing and Proposed Schemes

Decryption Time (in ms)	
Existing Scheme	**Proposed Scheme**
11.5	8.8

The decryption time for the existing method and the proposed method is compared, and the resultant graph is shown in figure 5. The decryption time of our model has been measured to be 8.8ms in comparison to 11.5ms of the existing scheme. This shows an improvement of approximately 24 per cent.

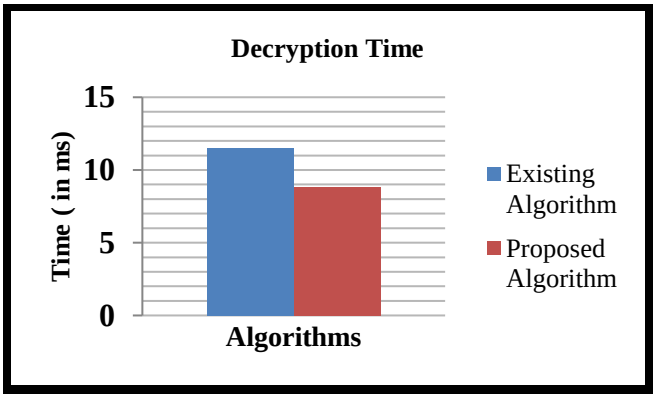

Figure 5 : Comparison of Decryption Time of the Existing and Proposed Models

From figures 3, 4 and 5 given above, it is evident that the key generation time, encryption time, and decryption time required for the proposed method is less when compared to the existing method, and hence the processing of the authentication and payment transaction is achieved in a reduced time interval. Thus, the superiority of the proposed research method is proved experimentally.

Total Time

The total time required by the existing method for the complete cryptography process along with the proposed method is given below in Table 4. It is clear from this data that the method proposed in this research work has gained a significant upper hand as far as the time taken for the complete cryptography process is concerned. The data shows that there is an overall improvement of approximately 27 per cent in the total time taken by the method proposed. This can be depicted in the form of a graph as shown in figure 6.

Table 4: Total Time Taken by the Existing and Proposed Methods

Total Time (in ms)		
Time	**Existing Algorithm**	**Proposed Algorithm**
Key Generation	6.5	4.2
Encryption	10.2	8.2
Decryption	11.5	8.8
Total	**33.2**	**24.3**

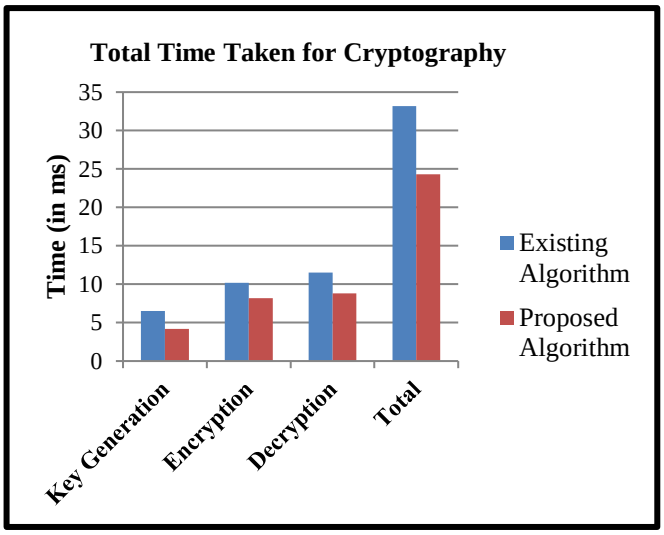

Figure 6: Comparison of Total Time taken for Cryptography by the Existing and Proposed Methods

The performance of the proposed model is evaluated on four parameters namely, key generation time, encryption time and decryption time. The proposed model has been shown to consume around 27 per cent of the time for the whole process of cryptography in the proposed model as compared to that of the existing model. The results prove beyond doubt the superiority of the proposed model over the existing model.

VI. CONCLUSION AND SUGGESTIONS

With the growth of the Internet and smartphones, mobile computing is growing at a tremendous pace. Mobile phones are being used as wallets to store confidential documents and to effect financial transactions using various applications through Cloud Computing. The present paper focuses on the critical issue related to security in the cloud i.e. secure financial transactions. A Cloud Server is proposed to facilitate the user in making financial transactions by keeping track of all the processes through a database. Further, a payment gateway is also integrated with the framework to achieve the desired financial transaction. The experimentation of the proposed research work is implemented and validated in the Java platform. Several parameters were evaluated in the performance evaluation section to decide the superiority of the proposed method. The performance evaluation metrics of the present scheme are compared with existing schemes. The comparative results obtained for the proposed method and the existing methods show the efficiency of the proposed method. A total time saving of approximately 27 per cent has been achieved in the process of cryptography considering it to be comprised of key generation time, encryption time and decryption time. The implementation of the work is done in a different environment with different strategies that get the bright idea of the research and reduces the security threats in work. This method improves the security of the network, and the data transfer remains protected with this model. This work is intended for improved results to classify/identify secured and unsecured data.

The proposed method is at the intersection of cryptography, authentication, financial transactions and security in general. The future research suggestions for this proposed research work are given as follows:

- The use of two keys, i.e. public and private keys, can be made to encrypt and decrypt confidential data at the user end and cloud end.
- Incorporation of the classification algorithms, which include C 4.5, Regression-based and decision tree-based classification can be done.
- The use of biometrics, along with other security tools for authentication, can be used to attain higher levels of security.

VII. REFERENCES

[1]. W. T. Meshach and K. S. Babu, “Secured and efficient authentication scheme for mobile cloud,” International Journal of Innovations in Engineering and Technology (IJIET), 2(1), pp. 2319-1058, 2013.

[2]. L. Cheung and C. Newport, “Provably Secure Cipher text Policy-ABE,” In Proceedings of the

14th ACM conference on Computer and communications security, pp 456–465, 2007.

[3]. X. Li, "Cloud Computing: Introduction, Application and Security from Industry Perspectives," International Journal of Computer Science and Network Security, vol. 11, pp. 224-228, 2012.

[4]. R. Chowdhury and D. De, "Secure Money Transaction in NFC Enabled Mobile Wallet Using Session Based Alternative Cryptographic Techniques," in Computer Information Systems–Analysis and Technologies, Springer Berlin Heidelberg, pp. 314-323, 2011.

[5]. W. Chen, G. P. Hancke, K. E. Mayes, Y. Lien, and J. H Chiu, "NFC Mobile Transactions and Authentication Based on GSM Network," in 2nd International Workshop on Near Field Communication NFC, IEEE Press, pp. 83–89, 2010.

[6]. S. Grunberger and J. Langer, "Analysis and test results of tunnelling IP over NFCIP-1," in First International Workshop on Near Field Communication, IEEE Press, Hagenberg, pp. 93–97, 2009.

[7]. J. T. Isaac and J. S. Camara, "A secure payment protocol for restricted connectivity scenarios in m-commerce," in E-Commerce and Web Technologies, Springer Berlin Heidelberg, pp. 1-10, 2007.

[8]. J. Gao, J. Cai, K. Patel and S. Shim, "Wireless Payment," Proceedings of the Second International Conference on Embedded Software and Systems ICESS'05, pp. 367-374, 2005.

[9]. Sherman, M. (2014), "An Introduction to Mobile Payments: Market Drivers, Applications, and Inhibitors," MOBILESoft2014, 1st International Conference on Mobile Software Engineering and Systems pp.71-74,June 02-03,2014, Hyderabad, India, 2014.

[10]. M. L. Das and N. Samdaria, "On the security of SSL/TLS-enabled applications," Applied Computing and Informatics," vol. 10, issues 1–2, pp. 68-81, 2014

[11]. S. M. Shedid, and M. Kouta, "Modified SET protocol for mobile payment: An empirical analysis," International Conference on Software Technology and Engineering, vol. 1, pp. V1-350 – V1-355, 2010.

[12]. X. Yong and L. Jindi, "Electronic payment system design based on SET and TTP," International Conference on E-Business and E-Government, pp. 275 – 278, 2010.

[13]. S. Kadhiwal and M. A. U S Zulfiquar, "Analysis of Mobile Payment Security Measures and Different Standards," Computer Fraud & Security, vol. 07, no.6, pp. 12–16, 2007.

[14]. R. Patel, A. Kunche, N. Mishra, Z. Bhaiyat and R. Joshi, "Paytooth - A Cashless Mobile Payment System based on Bluetooth," International Journal of Computer Applications, vol. 120, no. 24, 2015.

[15]. S. Swarnalatha, S. Uma, R. Yugha and P. Sindhuja, "A survey on Securable mobile payment systems in mobile commerce," International Journal of Engineering Research Online, vol. 3, issue 2, 2015

[16]. SPA (2015), A competitive market for interoperable mobile wallets, Available at http://www.nfcidea.pl/wp-content/uploads/2015/05/A-competitive-market-for-interoperable-mobile-wallets.pdf, accessed on 19th June 2016.

[17]. R. Joshi, "Financial Inclusion through Mobile Wallet," National Seminar on Application of Information and Communication Technology (ICT) for Innovation in Business, India, March 5, 2016, 2016.

[18]. P. Yadav, "Active Determinants For Adoption Of Mobile Wallet," i-manager's Journal on Management, vol. 12, no. 1, pp. 7-14, June-Aug. 2017.

[19]. Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences 387, pp. 103-115, 2017.

[20]. Fang-Yie Leu, Yi-Li Huang and Sheng-Mao Wangv, "A secure m-commerce system based on credit card transaction," Electronic Commerce Research and Applications, vol.14, 2015.

Cite this article as :

Sunil Mankotia, "A Secure Payment Method for Mobile Wallet Framework", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 4, pp. 710-721, July-August 2022.
Journal URL : https://ijsrst.com/IJSRST229542