2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) | 979-8-3503-8247-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/UPCON59197.2023.10434601

Enhancing Security Of Mobile Payment Applications Using Block Chain

[1]Lipsa Das
Amity School of Engineering and Technology, Amity University,
Greater Noida, UP, India
lipsaentc9@gmail.com

[2]Chamandeep Kaur
Dept. of Computer Science and Information Technology
Jazan University
Jazan, KSA
kaur.chaman83@gmail.com

[3]Ayasha siddiqua
Dept. Of Information technology and Security,
Jazan University, Jazan, KSA
asiddiqua@jazanu.edu.sa

[4]Durdana Taranum
Computer Science & Information Technology Department,
Jazan University,
Jizan, Kingdom of Saudi Arabia
durdana.07@gmail.com

[5]Ganesh Vasudeo Manerkar
Department of Information Technology,
G.E.C. Farmagudi, Ponda, Goa
gvm@gec.ac.in

[6]Ajay Rana
Amity School of Engineering and Technology, Amity University,
Greater Noida, UP, India
ajay_rana@amity.edu

***Abstract*: Authentication, access control, confidentiality, integrity, on-repudiation, and vacuity come obligatory security Mobile Payment operations. The authentication process consists of two-way including stoner verification and origin verification. Authentication consists of two ways which includes validating the stoner and determining the provenance of the data source. Access control can give authorized individualities access to the payment system while precluding unauthorized people from penetrating the payment system. To avoid unresistant assaults on sale data, the information must also be kept nonpublic. The vacuity of the payment system guarantees that it's accessible. Data integrity prevents data from being tampered with, and non-repudiation verifies that the communication was transferred by a specific stoner. This paper describes a new security medium to ameliorate data integrity during the sale using a mobile payment operation.**

Keywords: Authentication, Data integrity, block chain, confidentiality, non-repudiation

I. INTRODUCTION

A mobile payment application is one that serves as an alternate payment method for payment through cash, checking the payment process through credit card or bank details. It enables us to complete the purchase entirely from our mobile phone. Mobile payment does not replace traditional physical payment methods, despite its recent advancements. Few of the mobile payment applications considered for the survey include Google pay, BHIM, Apple pay, Samsung pay, Amazon pay, Payzapp, Paytm.

A. Impact of mobile payment applications

Since it sends off in August 2016, UPI has been seeing exceptional development with regards to add up to number of clients, limit, and exchange esteem [1]. At present, 150 banks have a UPI stage, and another 100 PSP UPI applications are accessible on application revelation stages. In no less than a time of UPI's starting, around 20 million individuals have enrolled for an assortment of UPI PSP applications. Since its commencement in September 2017, the general worth of Computerized exchanges has grown up to 182 percent consistently, with a complete oversaw measure of Rs. 287 billion. The month-to-month volume of exchanges on UPI has now outperformed the month-to-month volume of exchanges of all e-wallets in India. UPI exchanges are presently less important than credit and check card exchanges, which produce around Rs.2700 billion every month, except UPI is developing at a quicker pace.

Today, India has 1.18 billion portable associations, 700 million web clients, and 600 million cell phones, with a quarter-by-quarter increment of 25 million [2]. In India, 69 %of grown-ups have their own cell [3]. The UPI stage currently has 100 million month to month dynamic clients, with an objective of 500 million by 2025.[4] The portion of UPI exchanges in by and large volume of computerized exchanges expanded from 23% in 2018-19 to 55% in 2020-21, with a typical exchange worth of Rs 1,838.UPI was initially presented in 2016, when it was tested by the Public Installments Organization of India and sent off by 21 part banks under the administration of Raghuram G. Rajan, then legislative head of the Hold Bank of India. UPI's interest group incorporates each and every individual who consolidates advanced installment techniques to send cash.

B. Workflow of mobile payment application

Verification, access control, privacy, uprightness, non-disavowal, and accessibility become compulsory security Portable Installment applications. The validation cycle comprises of 2 stages including client confirmation and beginning check [5]. [6] Authentication comprises of two different ways which incorporates approving the client and deciding the provenance of the information source. Access control can give approved people admittance to the installment framework while keeping unapproved individuals from getting to the installment framework. To stay away from aloof attacks on exchange information, the data should likewise be kept private. The accessibility of the installment framework ensures that it is available. Information respectability keeps information from being altered, and non-renouncement checks that the message was sent by a particular client.

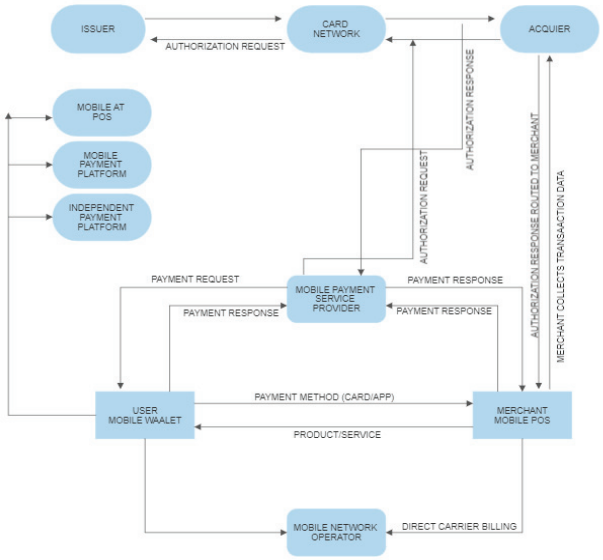

Fig. 1. Workflow of mobile payment application

C. *Various payment modes in mobile applications*

TABLE I. MOBILE FINANCIAL SYSTEM [8]

Characteristics	Symmetric Key	Public Key
Several keys are used for encryption, and de-cryption	The same key is used for encryption-decryption	Two different keys are used for encryption and decryption
Speed of encryption and decryption	Faster than public-key encryption	Slower than symmetric key encryption
Size of ciphertext	Usually less than or same as the plain text	More than plain text
Key exchange	A big problem	No issue
Key usage	Used for confidentiality but not for digital signature	Used of confidentiality and digital signature as well

- Mobile Payment: Mobile payment refers to a payment system wherein an individual utilizes a mobile device to authorize, initiate, and confirm a transaction.
- Mobile Wallets: Mobile Wallets is a smartphone app with the following functionalities that can take the place of real wallets: The capacity to keep track of payment details, membership cards, and other marketing strategies [7].
- Mobile Banking: Mobile banking involves delivering a range of banking services through mobile phones, encompassing both financial and non-financial transactions. This convenient and accessible approach allows individuals to perform various banking activities using their mobile devices, offering a seamless and user-friendly experience for managing both financial transactions and related services.

1) *Net Banking*

It is a computerized technique to go through with financial exchanges through the internet. It fundamentally decreases the bank working expense and offers extraordinary comfort to clients. The course of installment through net banking is portrayed as follows.

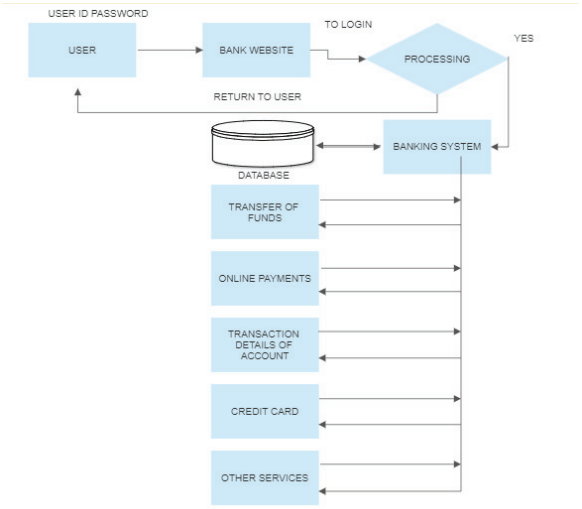

Fig. 2. Flow of Netbanking

2) *Aadhar enabled payment service (AEPS)*

AEPS is a bank-drove idea that empowers online interoperable monetary exchanges at PoS (Retail location/Miniature ATM) using Aadhaar verification through any bank's Business Reporter (BC)/Bank [9].

The functioning component of AEPS machines is like a retail location framework. Rather than a charge/Visa pin, the retailer should enter the client's Aadhaar number and affirm the exchange utilizing the client's biometric information.

The following information is required to initiate an AEPS transaction.

- The bank's name or the IIN (Issuer Identification Number).
- Fingerprint
- Aadhaar Number

3) *Electronic Clearing System (ECS)*

The Electronic Clearing Framework (ECS) [10] can be utilized to send cash starting with one ledger then onto the next electronically. It is broadly utilized for institutional installments like profits, interest, compensations, and annuities. ECS can likewise be utilized to cover bills and different charges, like telephone, energy, and water charges, or to make comparable regularly scheduled payment installments on advances and Taste ventures.

4) *NEFT (National Electronic Funds Transfer)*

The Public Electronic Assets Move (NEFT). [11] It is an electronic installment framework that empowers balanced moves across nations. Clients can utilize this help to electronically move assets from any bank office in the country to any individual who has a record with another NEFT-empowered bank office. You can likewise utilize web banking and versatile banking to make NEFT moves.

5) RTGS (Real Time Gross Settlement)

RTGS installment frameworks are experts in reserve move where the exchange of cash or security happens from one bank to some other bank on a "constant" and on a "gross" premise. It is principally intended for high value-based sums [12].

6) Immediate Payment Service (IMPS)

IMPS gives a dependable, 24-hour interbank electronic asset move administration utilizing cell phones[11]. Pixies is a complex approach to rapidly moving installments between banks in Asian nations through portable, web, and ATMs that are secure as well as effective in both monetary as well as nonterms.

7) ONE TAP

One tap Installment [13] is a method for paying web-based that makes installments at ease. It utilizes short reach remote innovation to make secure installments between contactless chip card or installment empowered versatile/wearable gadget and a contactless empowered checkout terminal.

8) NFC (Near Field Communication)

NFC installments are contactless installment strategies that utilize Close to Handle Correspondence (NFC) [14] innovation to move information among peruses and installment gadgets. NFC installment utilizes cell phone applications, for example, Google pay, BHIM, Paytm, Phonepe, and other e-wallet applications, and numerous others. The NFC component may likewise be utilized for one-tap installments, which can move reserves by means of e-wallets installments through.

9) Electronic purses/wallets

E.wallet is a wallet that might be utilized to make online installments utilizing a cell phone. An e-wallet works in basically the same manner to a credit or check card. To make the installments, the singular's ledger needs to be linked to an e-wallet. The essential goal of an e-Wallet is to empower paperless cash exchanges.

D. Types of e-wallets

Relying upon the idea of the business and the end-clients, there are a few kinds of e-wallets that carry out different roles. The assortments of e-wallets that backers give to their end-clients to explicit capabilities are recorded underneath [15].

1) Closed wallets

Clients can utilize a shut wallet to make installments utilizing an application or a site.

They are normally made by organizations that offer items and administrations to their clients.

The put away subsidizes in a shut wallet must be utilized to finish exchanges with the wallet's guarantor. Outside installments are impractical with shut wallets.

2) Semi-closed wallets

Users use a semi-shut wallet to perform exchanges at traders and areas that are listed. Semi-shut wallets just have a restricted covering area. To acknowledge installment from the wallet, shippers should initially acknowledge the agreement or concurrence with the backer.

3) Open wallets

Open wallets are given by banks. Users that have open wallets can get to them for a transaction. Payments can be made whenever both on the web and at the store. Open wallets give you the adaptability to move reserves at whatever point and any place the clients need. Clients of the open e-wallets can go through with exchanges from anyplace on the planet, however both the source and the beneficiary high priority autonomous records on a similar application.

4) Crypto wallet

Users' public and confidential keys are put away in crypto wallets. Hardware wallets, otherwise called cold wallets, are intended to give an additional layer of safety and protection. Offline wallets can be worked with a USB stick. These wallets can be utilized to make digital money installments [16].

5) IoT wallet

The Web of Things (IoT) alludes to an organization of interconnected gadgets. These can be found in watches, coats, wristbands, and other wallet-empowered items like savvy vehicles, shrewd fridges, and that's only the tip of the iceberg. E-cash and virtual monetary forms are acknowledged by means of IoT wallets [17].

6) UPI payment

Brought together Installment Connection point (UPI) is an easier technique for making electronic installments wherein exchanges are directed without giving check card numbers, CVV, pin numbers, client names, or other data [18]. The Brought together Installments Connection point (UPI) is a surprisingly quick installment framework planned by the NPCI, which is represented by the RBI. Public Installments Partnership of India is truncated as NPCI. With a real ledger and UPI PIN, two multilateral gatherings can take part in a quick cash move. All bank exchanges are verified and approved utilizing the UPI PIN. It works 24 hours per day, seven days per week, paying little heed to bank working hours. Each exchange requires the contribution of a payer account number and a payee account number for store move. One record and a UPI pin can make the installment framework run all the more easily.

II. MOBILE PAYMENT SYSTEM SECURITY MECHANISM

Numerous security strategies have been executed to guarantee the security of versatile installments. These techniques are illustrated below.[19]

- Apple Pay and Samsung Pay both acknowledge fingerprints. The capacity to utilize a unique finger impression to affirm an installment by simply putting a finger on the finger impression scanner the gadget
- Username/secret phrase: Usernames and passwords are much of the time utilized by versatile installment stages and independent portable installment frameworks to verify client personalities and permit buys.
- Multifaceted confirmation: To validate clients, a few versatile installment frameworks utilize multifaceted verification. At the point when a client signs into the help with another telephone, for instance, a validation code is required. The verification code is in this

manner conveyed to the client's enrolled email address by means of email.

- SSL/TLS: SSL/TLS are much of the time used to get information sent over the Web. At the point when portable installment information goes over the Web, SSL/TLS can ensure secrecy, respectability, and validation.
- Secure Component: The safe component on a cell phone is likewise utilized by NFC-based versatile installment frameworks to safeguard delicate information and for cryptographic handling.

In Apple Pay, for instance, fingerprints and other delicate data, for example, the gadget's novel record number, are saved in the protected component.

Encryption technologies, authentication, and a firewall are part of the mobile payment system security process.

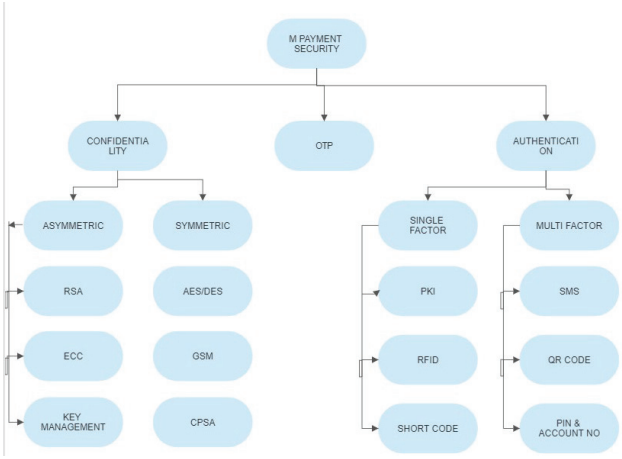

Fig. 3. M Payment Security

A. *Symmetric Key Encryption (SKE):*

The SKE[20] system operates by encrypting communications using a shared key. This implies that both the sender and the recipient utilize a single key for both encryption and decryption processes. Prior to the actual data transfer between these parties, the common key is securely exchanged over a protected channel, ensuring a confidential and secure means of communication. This method establishes a shared understanding between the communicating entities, allowing for the secure exchange of information with the assurance that the shared key remains confidential during the encryption and decryption processes.

B. *Public-Key Encryption (PKE):*

The PKE [21] system is classified as an asymmetric encryption method, distinguishing itself from symmetric key systems by employing distinct keys for encryption and decryption processes. In the PKE system, two unique keys, namely the public key and the private key, are utilized. The public key is shared openly and used for encrypting messages, while the private key is kept confidential and employed for decrypting the received messages. This dual-key mechanism enhances the security of communication, as the information encrypted with the public key can only be decrypted by the corresponding private key, providing a secure and reliable means of protecting sensitive data in digital communication..

C. *Authentication*

Authentication included: Digital signature and certificate authority.

III. Comparison of Encryption Methods [22][23]:

A. *Digital Signature:*

Computerized signature (DS)[24] is a string esteem determined utilizing text worth to a Hash esteem. DS is utilized to confirm the beginning of the got text and demonstrate whether they got text is with next to no changes. To ensure the accessibility of DS, PKI is regularly utilized. It proposes a total arrangement of safety confirmation and observes different public key encryption guidelines for various areas like internet banking, e-banking, e-government, and web-based business protections.

B. *Certificate Authority*

The Certificate Authority (CA) is a believed association that distributes and oversees network security public keys foundation (PKI) and qualifications for message encryption. As a feature of the PKI, the CA will involve the library for verification. Clients reserve the option to check the data in the computerized certificate given by the candidate. Assume RA (Register Specialists) verifies thecandidate's information and issue a computerized certificate. Imparts clients are answerable for dispersing.what's more, denying certificates. Contingent upon the PKI, upon demand, the certificate may contain the holder's public key, the certificate, the name of the certificate holder, and other data about the holder of the public key

IV. Conclusion:

This paper delves into a comprehensive exploration of the security features and challenges inherent in various payment applications and online transaction methods. The examination encompasses a detailed discussion on the impacts, threats, and potential attacks faced by mobile payment systems, elucidating their workflow and intricacies. By scrutinizing the security aspects of diverse payment technologies, this study aims to provide insights into the vulnerabilities and protective measures essential for ensuring a secure and resilient landscape within the realm of electronic transactions.

REFERENCES:

[1] A. B. M. U. . Younus Khan, Prabhat Chandra Gupta, “Expansion of Unified Payment Interface”, Annals of RSCB, vol. 25, no. 6, pp. 12491–12499, Jun. 2021.

[2] https://economictimes.indiatimes.com/news/india/indias-growing-data-usage-smartphone-adoption-to-boost-digital-india-initiatives-top-bureaucrat/articleshow/87275402.cms

[3] S. Karnouskos, "Mobile payment: A journey through existing procedures and standardization initiatives," in IEEE Communications Surveys & Tutorials, vol. 6, no. 4, pp. 44-66, Fourth Quarter 2004, doi: 10.1109/COMST.2004.5342298.

[4] Shree, Sudiksha, Bhanu Pratap, Rajas Saroy, and Sarat Dhal. "Digital payments and consumer experience in India: a survey based empirical study." Journal of Banking and Financial Technology 5 (2021): 1-20.

[5] C. G. Tekkali and J. Vijaya, "A Survey: Methodologies used for Fraud Detection in Digital Transactions," 2021 Second International Conference on Electronics and Sustainable Communication Systems

(ICESC), Coimbatore, India, 2021, pp. 1758-1765, doi: 10.1109/ICESC51422.2021.9532915.

[6] W. Liu, X. Wang and W. Peng, "State of the Art: Secure Mobile Payment," in IEEE Access, vol. 8, pp. 13898-13914, 2020, doi: 10.1109/ACCESS.2019.2963480.

[7] D'Silva, Derryl, Zuzana Filková, Frank Packer, and Siddharth Tiwari. "The design of digital financial infrastructure: lessons from India." BIS Paper 106 (2019).

[8] Sinha, Mona, Hufrish Majra, Jennifer Hutchins, and Rajan Saxena. "Mobile payments in India: the privacy factor." International Journal of Bank Marketing 37, no. 1 (2019): 192-209.

[9] Raghavan, Malavika. "Transaction failure rates in the Aadhaar enabled Payment System: Urgent issues for consideration and proposed solutions." Available at SSRN 3604119 (2020).

[10] Mer, Akansha, and Amarpreet Singh Virdi. "Modeling millennials' adoption intentions of e-banking: Extending UTAUT with perceived risk and trust." FIIB Business Review 12, no. 4 (2023): 425-438.

[11] Timilsina, Satyendra, and Ch Appa Rao. "A Comparative Study of NEFT and IMPS as Retail Payments Instruments in India." Think India Journal 22, no. 14 (2019): 9672-9681.

[12] Ansari, Elham Aijaz, and Twinkle Gupta. "A Study of Payment and Settlement Systems in India-Products, Growth and Future in Indian Banking Sector." Amity Journal of Insurance Banking and Actuarial Science (AJIBAS): 1.

[13] KUMAR, NIKHIL. "CONSUMER PERCEPTION ABOUT ONLINE PAYMENTS METHODS IN INDIA." PhD diss., 2022.

[14] HAMZAH, Muhammad L., Yenny DESNELITA, Astri A. PURWATI, Ermina RUSILAWATI, Rukun KASMAN, and Fahmi RIZAL. "A review of Near Field Communication technology in several areas." Revista Espacios 40, no. 32 (2019).

[15] Sikri, Alisha, Surjeet Dalal, N. P. Singh, and Dac-Nhuong Le. "Mapping of e-wallets with features." Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies (2019): 245-261.

[16] Suratkar, Saurabh, Mahesh Shirole, and Sunil Bhirud. "Cryptocurrency wallet: A review." In 2020 4th international conference on computer, communication and signal processing (ICCCSP), pp. 1-7. IEEE, 2020.

[17] Lomazina, Tatyana A., Tatyana G. Surovtsova, and Dmitrii A. Ivanov. "Development of a Cryptocurrency IoT wallet with Automatic Authentication." In 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp. 318-323. IEEE, 2021.

[18] Kumar, Renuka, Sreesh Kishore, Hao Lu, and Atul Prakash. "Security analysis of unified payments interface and payment apps in India." In 29th USENIX Security Symposium (USENIX Security 20), pp. 1499-1516. 2020.

[19] Patil, Pushp, Kuttimani Tamilmani, Nripendra P. Rana, and Vishnupriya Raghavan. "Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal." International Journal of Information Management 54 (2020): 102144.

[20] Lai, Yen-Lung, Jung Yeon Hwang, Zhe Jin, Soohyong Kim, Sangrae Cho, and Andrew Beng Jin Teoh. "Symmetric keyring encryption scheme for biometric cryptosystem." Information sciences 502 (2019): 492-509.

[21] Bradley, Tatiana, Jan Camenisch, Stanislaw Jarecki, Anja Lehmann, Gregory Neven, and Jiayu Xu. "Password-authenticated public-key encryption." In Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17, pp. 442-462. Springer International Publishing, 2019.

[22] Ahmed, Waqas, Aamir Rasool, Abdul Rehman Javed, Neeraj Kumar, Thippa Reddy Gadekallu, Zunera Jalil, and Natalia Kryvinska. "Security in next generation mobile payment systems: A comprehensive survey." IEEE Access 9 (2021): 115932-115950.

[23] Ma, Haiyun, and Zhonglin Zhang. "A new private information encryption method in internet of things under cloud computing environment." Wireless Communications and Mobile Computing 2020 (2020): 1-9.

[24] Lokhava, Marta, Giuliano Losa, David Mazières, Graydon Hoare, Nicolas Barry, Eli Gafni, Jonathan Jove, Rafał Malinowsky, and Jed McCaleb. "Fast and secure global payments with stellar." In Proceedings of the 27th ACM Symposium on Operating Systems Principles, pp. 80-96. 2019.