E WALLET: PAYMENT MECHANISM AND ITS SECURITY MODEL

Bhavna Galhotra[1*], Aman Jatain[2], Shalini Bhaskar Bajaj[3], Vivek Jaglan[4]

Abstract
An electronic wallet, sometimes known as an "e-wallet," is a software program that allows users to do financial activities online using computers or smart phones, such as making purchases, paying bills, transferring money, and booking flights. A relatively new idea, the electronic wallet has quickly ingrained itself into consumer culture. After Demonetization, e-wallet company customer bases experienced a sharp increase. Individuals can easily download an e-wallet app in the current environment to make their e-payments conveniently. The majority of individuals prefer using their mobile devices for both online and offline cash transactions since they are so convenient. Due to its distinctive favourable characteristics, it is attracting attention. This document attempts to provide answers to several operational concerns

[1*]Research Scholar, Computer science dept., Amity University, Asst. Professor
[2]Asst. Professor, Computer science dept., Amity University
[3]Professor & Head, Computer science dept, Dehradun
[4]Professor& Dean Research, Graphics Era University

***Corresponding Author**: Bhavna Galhotra
*****Research Scholar, Computer science dept., Amity University, Asst. Professor

DOI: - 10.53555/ecb/2022.11.6.137

I. Introduction

A financial tool (credit card or digital currency) is used to facilitate online eommerce activities su chas buying items, paying utility bills, transferring money, booking flights, etc. via smart phones or computers. This tool is known as an electronic wallet (e-wallet). [1]

Electronic wallets are a relatively new idea that ar e quickly gaining popularity among consumers. The customer base of ewallet companies experien ced a sharp increase after Demonetization.In the c urrent environment, it is simple for individuals to download anelectronic wallet app to conveniently make their e-payments. [2]

The majority of individuals prefer using their mob ile devices for both online and offline cash transac tions since they are so convenient.Due to its specia l beneficial attributes, it is attracting attention. This document attempts to answer specific questions about e wallet operational procedures, e wallet types, and e wallet security challenges. A system called E-wallet is used to save consumer information for quick access during online transactions. An e-wallet service can lessen the inconvenience for the customer since filling out documents for an online transaction can be a reason to cancel one. Most of the time, a cashless economy is necessary to replace all physical cash transactions with card or digital transactions in order to limit the circulation of physical cash. [3] Cashless transactions will be influenced by a variety of factors, including government intervention, new breakthroughs, and technological knowledge. E-wallets have witnessed a substantial trend in this area, moving directly from cash. A mobile wallet, a relatively new concept in India, has outperformed credit card usage and is gradually replacing traditional payment methods. It is essentially a virtual wallet where users may save money to use for mobile payments both online and off. Digital currency must be added to the e-wallet utilizing online banking or debit/credit cards. It drives the payment platform to improve point of sale wherever and whenever possible. The major goal of e-wallet businesses is to enchant their customers with simple methods of money transfer and transactional capabilities.

II. Objective of the study

The process of adding digital cash to an e-wallet, issuing institutions, and security concerns associated with e-wallet use, and other elements are identified and summarized in this article. To create an alternate method of paying with virtual currency that allows the user to physically and visually view their expenditures. Exposure to such elements offers insight into the acceptance of digital payment systems, which may call for further emphasis and awareness.

III. E wallet

An electronic wallet is a form of online account w here a user can keep money for upcoming transact ions. A password is required to access an E-wallet. One can pay for online purchases from websites se lling anything from physical things, services, and plane tickets using an E-wallet.[4]

Software and data are the two major components o fan e-wallet.
The software component secures and encrypts the data while storing personal information.
It offers a simple and secure manner of receiving p ayments for information supplied by the consumer , such as their name, shipping address, preferred p ayment method, required payment amount, credit or debit card information, etc.Wallets have been la unched by several businesses in the telecommunic ations and ecommerce sectors to promote the use of digital cash. [5]
The software component secures and encrypts the data while storing personal information.

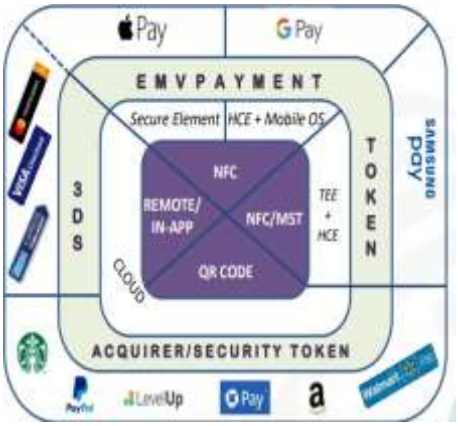

Figure 1 *EMV Payment Structure*

This article is conceptually based, and descriptive research methodology is utilized to offer the data needed to meet the objectives. A choice of information sources was made in order to conduct searches for pertinent material. Academic Search Complete, E Journals, and Web of Knowledge were the databases used. A thorough analysis of prior studies and literature has been conducted to determine the definition, various e-wallet kinds, the process for adding digital cash, benefits, and security concerns associated with e-wallets.[6]

IV. Process for loading digital currency

Debit cards or online banking are used to load money into electronic wallets. The required amount must be chosen in the wallet, and the instructions for adding money through credit card or savings account must be followed. Once the funds are loaded, they can be used to pay for a variety of expenses, including cell bills, recharges, power bills, online point-of-sale transactions, etc. The only need is that the recipients of the funds must accept the method of payment.

a. Steps to be followed

The usage of mobile wallet is subject to fees, which include registration costs and cash loading fees. These fees can be more expensive than those associated with online banking. However, the primary benefit of using an UPI transactions when purchasing online, the payment businesses make the user offers or concessions in the form of cash backs, etc.

Figure 2 *Steps for loading digital currency*

V. Security Concerns of the E wallets and the Payment UPI's

While downloading the applications and other important content there are certain parameters that give false notifications and also results in some malfunctioning of the data or the content stored in the hand held devices

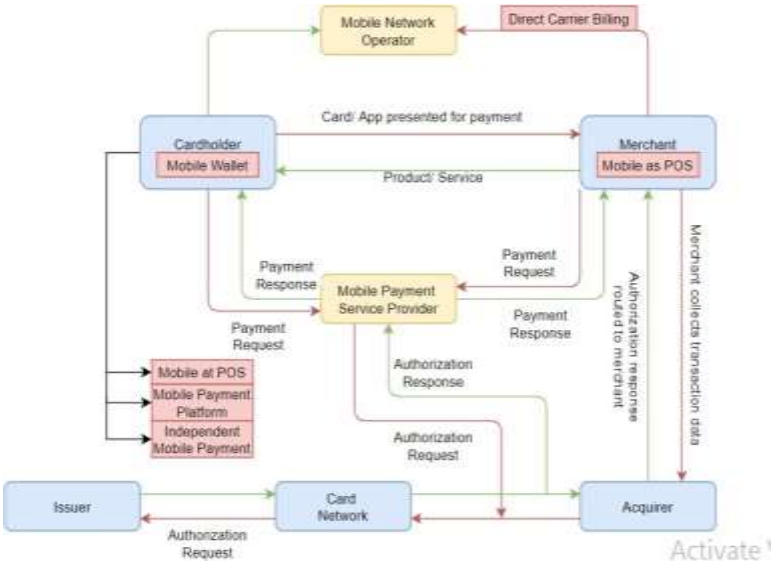

Figure 3 *Mobile Payment Model*

The suitable steps and the model that can be considered as the precautions

a. Confidentiality:

The user's transaction information, bank account information, and wallet balance should be kept private and inaccessible to unauthorized users or outside suppliers. We looked into whether the data (in-transit or saved data) was solely accessible to the targeted stakeholders to evaluate this aspect of the apps. [7]

b. Management of transaction non-repudiation: When it comes to mobile payments, transactions are confirmed via notifications, SMS, and emails that include crucial information (amount, time of transaction, sender, receiver, app vendor name, and comments), and these should be logged and tracked to prevent erroneous denial.

To assess this factor, we looked into:

- The transaction logs were kept up to date and if the information in the logs could be utilised in the event of a transaction repudiation [8]
- The app monitored transaction patterns and alerted users when they were out of the ordinary, such as when several transactions were carried out quickly (within a few seconds).
- Customer identification verification: It is crucial for mobile apps to confirm that the person transferring money is the verified account holder during a transaction.
- The usage of special passwords or the user's biometrics can both be used for authentication. To assess this element, we looked into Whether each transaction was authenticated and carried out with the approval of the parties involved. [9]
- The reliability of the login and logout processes. It would be the equivalent of leaving the door open for any burglar to enter the house whenever they wanted if this process is not sufficiently validated.
- Integrity of data and transactions: Customers should get accurate information about transactions and wallet balances in app notifications and statements. We looked into if the in order to assess this factor. The data that were kept and shown were precise and reliable. Processes used to validate transactions adhered to standards for trustworthy and dependable transactions. [10]
- Use and availability: In the case of mobile payment services, the network plays a crucial role in a customer's ability to use the services. Some mobile applications and USSD systems function through SMS or voice calls, making them accessible to users who do not have internet or data connections on their mobile devices.

We looked into the services

i. availability in a variety of formats and
ii. Dependability (such as the accessibility of information on the Ombudsman, security, and other topics) to evaluate this aspect.

- **Client data privacy:**

The payment app or service shouldn't request client information that breaches their privacy or puts them at risk for identity theft. This idea stands out in especially when installing an app and the user needs to grant access permissions to the program for a variety of fields. We looked into whether the

requested privileges were appropriate to analyse this aspect.[11]

- **Concerns with all the Applications over the transferring of the money**

Except for USSD, all mobile payment mechanisms had the potential for confidentiality breaches. This risk is greatest if the user misplaces or loses their mobile device, and it is even greater if the device is unlocked or not secured. Any information about transactions performed for Paytm, Free charge, I Mobile, and Bhim can be made public with unauthorised access to the phone. The one-time password supplied by a partner bank is accessible in an odd and unjustified way through the Paytm app. For all of the payment methods, there was insufficient management of the transactions to allow for repudiation in the future, if necessary. There was no indication that transaction patterns had been systematically examined to alert users to unusual or problematic transactions.[12]

Although the apps have authentication mechanisms enabled, we discovered that there are security issues. These security concerns appear if the user's phone is compromised, just like with confidentiality difficulties. Without the user's authorization, Paytm's partners, including Big Basket and Uber, are able to remove money automatically. This makes things easier, but it also permits unauthorized deductions (which can be challenged afterwards). I Mobile and Bhim both automatically log out users, however Paytm and Free charge do not, and logging out is also not simple for a new user. The latter two apps have this capability, which adds to the security against unauthorized use.

For the majority of the apps, data and transaction integrity was fairly good. The menu screen may vanish when using USSD if there is a delay in replying. The payment apps' assurance in this regard is a plus. Concerns include the fact that Freecharge displays an incorrect number and Paytm takes some time to refresh the balance amount.[13]

Unlike the other payment applications, USSD and Bhim may function on voice and SMS-based phone connections and do not require a data plan (internet access). They therefore make access more accessible. Both of these firms are clear about the process for resolving disputes, which is through an ombudsman, albeit this information can only be found by browsing websites for specifics rather than using the regular transaction screens.

All of the services analysed raise significant privacy issues. All of the apps demand access to the user's private data on the phone without making it obvious why this is necessary. Even when not using the QR way of payment, the apps do not work if the user restricts some access, such as access to the camera and media. Our responses consistently raised the issue. Because PhonePe had direct access to bank accounts and was actively launched and promoted, many respondents were unwilling to install it, and as a result, we were unable to include them in our study.

VI.Conclusion

Few recommendations for the model development

The users' trust will increase with improvements in data integrity (precision of balance sheet, transaction confirmation, and similar items) and confidentiality (ensuring that the data is only accessible to designated stakeholders). Urgent action should be taken to rectify some issues that were deemed to be major infractions, like allowing a merchant to deduct without the user's express authorization. The e-wallets lack clear instructions on the procedures needed to contact an ombudsman, in contrast to the USSD apps and bank apps. The developers of apps and Indian regulatory agencies must exercise due vigilance in this regard. The degree of security risk is inversely correlated with consumers' knowledge of security concerns, technology, and phone features. While user education is undoubtedly a strategy, it is advised that OS vendors and app vendors impose fundamental security hygiene as part of their design (such as requiring phone passwords, login passwords, logout, and similar practices).

Reference

1. I. Ames, “Fraud Detection in Mobile Money Transactions Using Machine Learning,” Business Analytics Commons, Lowa , 2019.
2. R. B. H. L. B. Alexander Schaub, “A trustless privacy-preserving reputation system,” no. DOI: 10.1007/978-3-319-33630-5_27, 2019.
3. M. P. Bosamia, “Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures,” in *IcSoftComp-2017*, Changa , India, 2017.
4. S. D. R. D. Abhipsa Pal, “Security in Mobile Payments:A Report on User Issues,” IIM banglore, March 2017.
5. N. Miriyeva, “SECURITY IN ELECTRONIC COMMERCE AND ONLINE PAYMENTS.,” in *16th Rome 2020 Conference Proceedings*, 2020.
6. D.P.K.S. Dr. Vandana Bhavsar, “Sustain-ability of Digital Payments: Empirical Evidence from India,” in *roceedings of the 2nd International Conference on Sustainability and Equity (ICSE-2021*, 2022.

7. P. O. G. Augustine Takyi, "Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce," *Contemporary Research on E-business Technology and Strategy,* pp. 232-239, 2012.
8. P. A., "Digital revolution, financial infrastructure and entrepreneurship: the case of India," *School of International and Public Affairs Columbia University New York,* Vols. 2019-01, 2019.
9. R. a. M. G. Singh, "Impact of digitalization on Indian rural banking customer: with reference to payment system," *Emerging Economy Studies-Sage Publication,* vol. 5, no. 1, pp. 31-41, 2019.
10. A. D. Bhavna Galhotra, "Impact of COVID-19 on digital platforms and change in E-commerce shopping trends," in *2020 fourth international conference on I-SMAC* , 2020.
11. A.J. Bhavna Galhotra, "Security Concerns for Mobile based Digital Wallets with the use of IDS &IPS System," *Test engineering and Management, 2020,* vol. 83, no. 3, 2020.
12. B. Galhotra, "Big Data: An opportunity and Challenge for M commerce," *2021 Fifth International Conference on I-SMAC* , 2021.
13. A.J. S. B. B. V. J. Bhavna Galhotra, "Mobile Payments: Assessing the Threats, Challenges and Security Measures," in *5th International Conference on Electronics (IEEE)*, 2021.