Security Aspects of Mobile Based E Wallet

G. Kanimozhi
Assistant Professor, Department of Computer Science
St.Britto's college
Chennai, India
e-mail:msajce.mcakanimozhi@gmail.com

K.S. Kamatchi
Assistant Professor, Department of Computer Science
St. Britto's college
Chennai, India
e-mail: kamshi26me@gmail.com

Abstract—An Electronic-wallet(e-wallet) is an electronic application that enables online e-commerce transactions like purchasing goods, paying utility bills, transferring money, booking flight etc. with a financial gadget (credit card/digital currency) using smart phones or computers. Electronic wallet is a very young concept that has taken on consumer psyche rapidly. Post Demonetization resulted in sudden surge in the customer base of e wallet companies. In the current scenario, it is easy for individual to download an e wallet app to make their e-payments conveniently. Since the transactions are done through mobile, it is preferred by most of the people for their online and offline cash transactions. It is gaining the attention due to its unique advantageous features. This paper tries answer for certain queries related to operational procedure of e wallet, kinds of e wallet and concluded with the security issues of e wallet.

Keywords*-E-commerce, Demonetization, E-Payment*

*****

I. INTRODUCTION*(E - WALLET)*

E-wallet is a system that stores a customer's data for easy retrieval for online purchases. Since completing forms of an e-retail transaction can be a reason for aborting a transaction, an e-wallet service can reduce this inconvenience for the consumer.Mostly cashless economy is required in order to replace all the transactions by using cards or by digital means in order to reduce the circulation of physical currency. Cashless transactions will depend on a number of categories such as technology awareness, new innovations and government intersession. For that, e-wallets have seen a notable track, which will move straight from cash to e-wallets.

A Mobile wallet, being a new concept in India, has been outperforming the credit card usage and is slowly beginning to replace the traditional payment methods. In simple terms, it is a virtual wallet where one can store cash for making online or offline payments through their mobile. E wallet must be loaded with digital currency by using internet banking, debit/credit cards. It propels the payment platform to enhance point of sales at anytime and anywhere. The main focus of e wallet companies is to enchant their consumers with easy money transfer solutions and transaction facilities.

II. OBJECTIVE OF THE STUDY

This paper identifies and synthesizes a number of factors such as digital cash loading procedure in e wallet, issuing agencies, security issues related to usage of e wallet etc., To produce an alternative form of paying with virtual money so the user can visually and physically see how much they are spending. Exposure to such factors provides an insight for accepting digitized payment system that may require increased emphasis and awareness.

III. ELECTRONIC WALLET

A. Data Collection

E-wallet is a type of online account in which a user can store money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for online purchases from websites selling anything from tangible products, services,and flighttickets. E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data. It provides an easy and safe way of purchasing (or) receiving payments of details provided by the customer which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc. Several company those in the e commerce and telecommunication services have introduced e wallet to encourage digitized mode of cash transaction.

B. Methodology

This article is conceptual based and descriptive research methodology is used to present data required to fulfill the objectives. In order to perform searches for relevant literature, a selection of data sources was made. The databases that were used are academic search complete, E journals, web of knowledge. An extensive study of previous research and literature, has been done to find out the meaning, types of e wallet, digital cash loading procedure, benefits and security issues related to e wallet.

C. Digital cash loading procedure

E wallets are loaded with money using debit cards or net banking. One has to select the amount needed in in the wallet and follow the instruction to load money through savings bank account or through credit card. Once the money is loaded it can be used to pay for number of transactions such as mobile bills, recharge, electricity bill, online point of sales etc., the only condition is that the vendors to whom the payment is made has to accept the mode of payment.

STEPS INVOLVED IN DIGITAL CASH LOADING

There are charges for use of mobile wallet which includes registration fees and cash loading charges. These charges are at times higher than those of internet banking. However, the main advantage with the e wallet is that while shopping online, the user gets concessions / offers from the payment companies in the form of cash backs etc.,

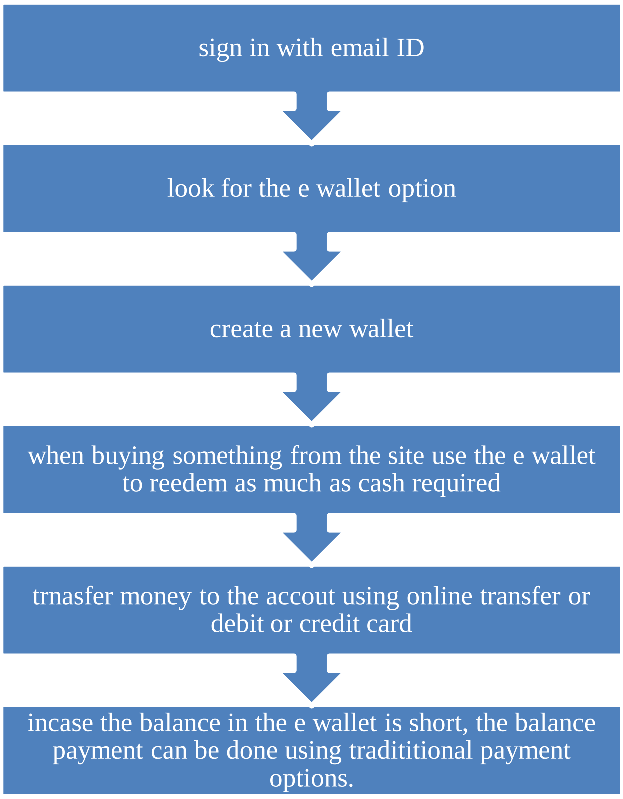
sign in with email ID
look for the e wallet option
create a new wallet
when buying something from the site use the e wallet to reedem as much as cash required
trnasfer money to the accout using online transfer or debit or credit card
incase the balance in the e wallet is short, the balance payment can be done using tradititional payment options.

Table 1 : steps involved in digital cash loading.

IV. KINDS OF E WALLET

E wallets are real cash in digital form. Post demonetization has paved way for existence of number of e wallets.Wallets are growing rapidly as they help in speedy transactions, especially for the e commerce companies. As such all the ecommerce market places have tied up with mobile wallets. Based on the source of issuance and purpose, e wallets are categorized as,

- ➢ Open wallets- refers to the wallets that have been issued by the banks
- ➢ Semi closed wallets- refers to the wallets that have been issued by telecom companies
- ➢ Closed wallets – wallet issued by wallet companies which work independently.

  There are number of e wallets that have been tied up with various vendors across India.

Kinds of e wallet		
Open wallets	***Semi closed wallet***	***Closed wallets***
State Bank Buddy	Idea money	ApplePay
LIME by Axis bank	Reliance Jio wallet	GoogleWallet
Chillr by HDFC	M – Pesa by Vodafone	AndroidPay
ICICI pockets	Airtel money	SamsungPay
Citi MasterPass	Jio money	Paytm
		Freecharge

V. SECURITY ISSUES OF CLOSED E WALLET

A. Handle with caution against Cyber Crime

Cyber security experts foresee large scale attacks on mobile phones and personal computers.

A clear majority of those who are downloading the apps are either uneducated or not aware of the ways of the cyber criminals. Their phones might be hacked as they unknowingly download some malicious gaming or such other app. following are the points to be remembered while using an E Wallet,

- Do not share the banking account passwords with others
- Avoid downloading game app or other app outside the play store as their online activity is tracked.
- Do not expose the mobile device to malicious websites and phishing attacks where the hackers can copy the security code.
- Do not lose your phone
- Install a basic antivirus and a malware scanner to overcome security threats.
- Do not store credit card details in the mobile phone.
- Keep your memory card clear and don't use others
- Be judicious about clicking on the links that could lead to malware. Free download and porn sites are notorious.

B. Cyber Security Measures

Security protection for E wallet is given in two ways:

- ➢ Secure socket layer (SSL): SSL is a computer networking protocol for widely used in internet secure service system which ensures trust between online purchaser and end user. It has about 90% share of security measures which is similar to credit cards security. It provides an authentication of buyer and merchant. This system also ensure the security which indentifies purchaser and also checks the customer using digital signature, finger prints, passwords, etc. , Data integrity keeps all the details confidential during the electronic transaction.
- ➢ Secure Electronic Transaction (SET): It ensures the security of confidential transmissions and digitized financial transactions. It is an alternative, more complex security system based on digital certificates and signatures among the purchaser, a merchant and a purchaser's bank. With the wide usage of electronic payment system it has gained much significance in security alerts.

C. Apple Pay

Apple pay is a Apple's solution for a digital wallet and mobile payment service using ios devices that allow the users to make payments in ios apps, web and in person. It digitizes and replaces the card (debit & credit) to store encrypted information about the payment in order to enhance security and to generate a dynamic security code that is used in EMV-mode is a magnetic strip based data emulation method of transaction to include dynamic card verification value (DCVV) during the transaction. EMV is a Europay, MasterCard, and Visa, that was originally created by the three companies. It is often called a Signature cards, PIN, a chip, that depends on the authentication methods that are employed by the card issuer.

It hides the track usage details between banks, the vendors and the customers. It replaces the customer's

Permanent Account Number (PAN) with a tokenized Device Account Number (TDAN) in order to hide the transaction details from the retailer by using EMV-payment tokenization method.

Apple pay request the user to authenticate the device to proceed with the payment. It creates a unique value to check the transaction is arrived from an authorized device. This distinctive identifier along with its cryptogram and token (DAN) involves the transaction to authorize and it cannot be used from another device even if the token is stolen because the token must come from the registered device. The authentication includes PIN number and finger print identification method using sensor(Touch ID).Finger print authentication provide security in case of stolen device that enhances high level of customer satisfaction.

Apple pay provides services that compatible with the devices include 6 Splus, ipad pro, iphone 6, and the Apple watch.

Data integrity

To provide data integrity for existing records generated by a trusted device refers the data stored in the database including metadata to track the origin of each unique customer data record. The Meta data has an application identifier to identify which app is used to store the customer data record. A digitally signed copy of the customer data record is available in the possible metadata to ensure integrity of customer details during the transaction.

Data Security

A highly Secure Element (SE) is a secure chip available inApple devices is a tamper evident e.g., the device automatically blank the memory to make sure that no keys can be extracted if it detects any trial of reading its contents. The terminal converse directly through the Near Field Communication (NFC) controller with the Secure Element over a dedicated hardware bus and the payment authorization details are never exposed to the application processor and it is localized to the local NFC field.

D. Google Wallet

Google wallet stores the encrypted user data in the Secure Element as its trusted store of sensitive payment information. The Secure Element (SE) chip is separate from the device (phones) components like memory, hardware and operating system. It allows only trusted programs to access the particulars like Google Wallet that is stored within. It is designed mainly for the region of customer retail. A user must unlock the phone, to enter the applications unique Personal Identification number between the merchant by tapping the device against a compatible card reader during the transaction. At last, the merchant receives a printed receipt with the confirmation on the point of sales terminal in order to receive the confirmation in the users mobile device.

Now days Google using Host Card Emulation based payment credentials in which the data are stored in the cloud. For transition from SE to HCE, Google focus on integration with other apps, authentication process, and loyalty rewards. The wallet controller released the Wallet app on a user’s device to store information in the timeline with contactless payment functionality and current state of the application.

Authentication

It offers a number of authenticate methods to the customers before any payments. It accepts PIN number, password and fingerprint authentication or a pattern to process the transaction. The tokens are loaded into the device prior before made the payment. When the connectivity is available then the tokens are sent by the Google server.

Data Protection

The users data stored on any device is vulnerable (in case of stolen device or compromised service by attack) it is essential to store the card sensitive data base in a secured cloud environment.

Finger print can validate the device profile tokens to reduce the risk by replacing the PAN with limited data during the payment system. Security keys are limited to prevent the misuse during transaction. It checks the transaction risk analysis.

Data integrity

It is mandatory for the users to register about their cards (Credit /Debit) with Android Pay. Android Pay (and Google) is free from the responsibility of identifying the user to the customer’s bank. The card issuer provides a number of verification methods to decide whether the user identity is verified.

1. The customer’s bank will send an email/text with a verification code to the user. 2.
2. The customer could call the bank and request the verification code.
3. If the customer installed with the bank’s application on the mobile, it is possible to sign in to verify the card to the app. This verification process will require a small charge. So the user needs to log on to the electronic banking system to provide the verification code.

The user enrolling a card on Android Pay needs to be aware that the card number is going to be transmitted and stored in Google’s cloud server.

E. Android Pay

Android pay is a digital wallet to enable users to make payments with Android phones, tablets or Applewatches and it is developed by Google. Android Pay uses near field communication (NFC) to facilitating funds transfer, it allows to transmit card information to the retailer. It replace the card (credit / debit card), or magnetic stripe transaction to upload the same in Android Pay wallet with point-of-sale terminals (POS). It provides two-step authentication method. The service allow Android devices to communicate with point of sale (POS) systems wirelessly by using a near field communication (NFC) antenna, Host-based card emulation (HCE), and Android's security.

Security

It locks with a new password or wipe all the personal information and data for a stolen device. It is recommended to use lock screen security. It waits for certain time to allow the user to unlock the device, if not it arise some security issues to delete all the personal details from the device. It uses a virtual account number to provide high-end security and easy to identify if suspicious activity happen and lock the screen automatically. Android Pay is supported by standard tokenization that will not be shared to the payment terminal during payment transaction via Android Pay. It does not send the credit/debit card number with the payment to a merchant, instead it generate a virtual account number to represent users account information to keep privacy in customers information, by sending a one-time security code instead of card/user details. It is available with Finger print identification in absence Android pay allows to access with pass code.

F. Samsung Pay

It is a mobile wallet application to make payments by influencing MST (Magnetic Secure Transmission) by emulating a magnetic card stripe reader. The user authenticates the Samsung Pay App and then the tokens are sent to the Point of Sale terminal (POS). Use of MST enables Samsung Pay allowable phones to make payment at magnetic stripe terminals and NFC tap-and-pay devices to extend their services in world-wide. Samsung Pay is closely related to the Samsung KNOX platform, which make available functionality for encrypted storage of payment tokens.

Authentication

In Samsung Pay, user authentication is done by the Trusted PIN Pad (TPP) or by the fingerprint scanner or, by both of which reside in Trust Zone. After successful authentication, customer's data are transferred to the respective payment network TA, then verifies the tokenized NFC or MST trusted app interface to execute the payment. The requests and responses for authentication are encrypted with keys to be recognized only by the intended TA recipients, within the TEE securely. To enhance security it is essential to erased the authentication decisions immediately after transmittal to prevent any single user authentication can attempt to perform multiple payments. Samsung Pay influences an additional security like Fingerprint authentication or for token assurance during token arrangement;it assigns a four-digit PIN Identity and Verification (ID&V). When Internet connection is avail then the tokens are provided in prior to the device. The issuer include the range for identifying device ID, one time passwords , billing address, (via SMS, email, and app-to-app) in order to choose the ID&V controls .

Data Integrity

TIMA (TrustZone-based Integrity Measurement Architecture) is a unique feature on Samsung mobile devices that effectively partitions memory and CPU resources into a "secure" and a "non-secure" world. TIMA, running in the Secure World, uses the TrustZone hardware to continuously monitor the integrity of the Linux kernel. TIMA forms a protection against malicious attacks on the kernel and core bootstrap processes with Secure Boot and Security development for Android (SE for Android). If kernel or boot loader integrity violations are detected, TIMA takes a policy-driven action, to disable the kernel at once and restart the device to a recognized state, thereby protecting all TIMA-dependent features, within the TEE from device-level attacks including Samsung Pay and the Samsung KNOX Workspace.

Data Protection

Data protection with TEE (Trusted Execution Environment) and Samsung KNOX relies on the device.. It provides a framework which effectively splits the hardware into two: Normal world and secure world. Both areas are isolated and only accessible via a Trust Zone monitor. TEE provides a range of hardware secure resources for key storage.PAN numbers are not installed on the smart phone and they are only made available to the issuer for payment. Therefore, it minimizes the risk of PAN (Permanent Account Number) leaks.

G. Paytm

Paytm is an electronic wallet acronym for "Pay through Mobile." It functions through the Paytm Wallet and payment gateway. It provides an easy of user interface to the customers. When money is transferred from bank to wallet, the banks generates and sends an OTP that is to be entered in the bank's portal to complete the transaction. However, Paytm picks up the OTP message that is not intended for Paytm and provide service through a browser, and an app is available on various operating systems like Windows, Android and ios. Paytm allows multiple payment modes for consumers to perform integrated bill payment transaction system.

Paytm includes a new security measure to add a lock on all transactions from the wallet. It ensures not only the phone but also provides a high layer of security for the Paytm application. This Paytm security feature includes Android's authorization mechanism, that allow users to access on a phone contains screen lock mechanism features like PIN, password, pattern, or fingerprint .

Security

Security in Paytm relies on a bank, transfer the payment with wallet money, the bank generates and issues an OTP to the customer. Paytm with its own popup it accesses this particular OTP. The device is used by more than an individual cannot maintain a secured data like SMS and email notifications in mobile wallets leads to a fraud transaction repudiations. Certain mobile phones with latest versions like Android and Apple ios allow fingerprint identification setup to provide high end security for every transaction. In Paytm it is not easy to find or logout the session immediately. It leads to the possibility for the hacker to do fraudulent transactions until the session expired. Customer must be careful to allow the transaction to be identified by a unique Transaction ID, which gives a sense of transparency and accountability. Easily readable monthly statement provides for transaction accountability. This is sent over email. Accurate data such as available balance, monthly usage data is not always available. Transaction confirmation SMS & email are provided immediately in line with reliable transaction procedures. Paytm require privileges such as access to user identity, media, camera, even though it is not mandatory for the current transaction. Without internet facility, money transfer is available through phone call and secured Paytm PIN.

H. Free charge

FreeCharge, a leading digital payments system allows consumers to buy a Google Play recharge code on its platforms. Customers use their FreeCharge app to select the 'Google Play' option on the website, and enter their details like mobile number, desired amount, make payment and receive a Google Play recharge code. Payment for these recharge codes can be done using FreeCharge for wallet balance, debit cards, credit cards, Net banking or UPI. The recharge code can be converted instantly through the "Redeem Now" link on the Google Play store.

Consumers can change the recharge code on the Google Play Store and at the time of requesting for the code by the user it is sent to the users registered email and through SMS on the mobile number registered by them.

Freecharge consumers will be able to purchase digital content by topping up on the Google Play Store like movies, games, e-books, android paid apps and so on.

The SMS and email notification is not highly secured in sharing the device. To provide security then the user is continuously logged in and no password is required for any transaction.

Free Charge never logs out the user automatically. It is not easy to find the logout option. There is no session timeout in the app. It allows for auto login to the app.

Transaction is not password-protected. These shortcomings could allow fraudulent transactions to occur, if the user is not careful. Unusual transaction patterns, though logged, are not detected and no warning is provided to the user. Will be an issue in case of fraud transaction repudiations Not linked to vendors, hence there is no concern of deducting money without explicit consent. Each transaction is identified by a unique Transaction ID, which gives a sense of transparency and accountability. Transaction confirmation SMS & email are provided immediately in line with reliable transaction procedures. The balance amount does not accurately reflect the available transaction amount. Though the app explicitly requests for privileges, it does not allow transactions without internet to access the phone, SMS and storage of user devices.

The FreeCharge wallet balance displayed in the home page of a user did not represent the transferable balance accurately. On clicking on it, a pop-up displayed that the amount was not usable cash balance but voucher balance. Voucher balance is not transferable and usable only for paying to certain third party vendors like mobile recharge, flight ticket booking, etc. However, the wallet balance display was misleading, giving a sense of available cash balance. In the latest Android and ios platforms, FreeCharge allows users to explicitly accept or deny access to privileges. However denying access to phone, SMS and storage caused installation failure and did not allow the user to carry out any transaction.

VI. KEY STEPS TO ENSURE SECURITY

A. Device screen is locked with strong code

The security measure is to set a lock screen code on the device. The attacker will face some problem in case of stolen device, there is a chance to steal your data, including mobile phone banking and e-wallet apps. Now a days inexpensive smart phones with Touch ID and fingerprint sensors facility in order to improve security and convenient to use. If the device without fingerprint sensors, it is necessary to set a pass codes and pattern locks to protect the device as well as the data and it should not be used elsewhere or shared with anyone.

B. Include App Lockers

There are numerous apps available that allow the users to set a passcode on other apps. It is mandatory to type a other password to unlock the app. Devices having an locker facility in their app it allows the user to handover the device to any person, without allowing the others to view the sensitive data. Some accepted app lockers are face-lock and Digi Locker, both of which have good appraisal on Google Play. If any situation occurs like to handover the device to any person, then allow the device settings to a guest mode option to provide high end security.

C. Keep a track of sent notifications

Whenever a transaction is made via users account, banks send an alert via SMS and email. It is mandatory to keep a track that ensures no one has to access any data digitally or otherwise. Apps such as Money View and Walnut can keep a record of transactions made on customers account by accessing SMS alerts from the user bank. If it is a registered net banking account from a secondary email ID, then it is essential, to set up an email forwarding mechanism to send notifications to the corresponding primary email ID. Otherwise, any important notification about misuse or hacked information might not be seen for hours or even days.

D. iPhones / Apps usage from unknown sources

Do not use iPhones or rooted Android smart phones to access your mobile banking applications and mobile wallets. The integrated security available in Google and Apple have used on the core OS to protect it from malware and hackers. Installing an app from unknown sources on Android, it makes the device vulnerable to attacks, and will allow hackers to steal your financial data remotely. Whereas the Google Play store and the App Store are relatively safer.

E. Avoid third-party keyboards

Third-party keyboards are used to store data and to access all the inputs given to the keyboards. It has a little un-secure for the banking applications and mobile wallets, given that the passwords and codes will also be visible. For security purpose the users does not store any personal data, it is needed to switch and work in the default keyboard while using sensitive apps.

F. Never use public Wi-Fi

Avoid public Wi-Fi networks, especially on a device that contain sensitive personal information or financial apps. Public Wi-Fi networks are usually unencrypted, for the users at risk of vulnerability, who could access and view all the data on your device, including your mobile payments applications.

VII. CONCLUSION

A. Conclusion

The impact of demonetization resulted in wide usage of plastic money, which works towards cash less economy. Mobile wallets are successful business ideas for start ups. It takes care of daily expenses without the need for having a single penny in the pocket. It has gained wide attraction due to its greater benefits than other payment modes. The RBI data revealed that there are about 20 million active users of e wallet in post demonetization. With efficiency and timesaving features, the size of mobile wallet market in India has grown significantly. According to the research firm RNCOS, the current Indian market size for e wallet stands at about Rs. 350 crores and it is estimated to rise to Rs.1210 crores by 2019. Ultimately e wallet contributes to digitization policy of the government which brings betterment in economy.

B. Future Direction

Digital IDs will be provided to specific accounts, wallets will update all information and to protect all legitimate users in an electronic commerce transaction. At that point, wallets will be universally distributed and invariably accepted.

REFERENCES

[1] Mia Olsen, Ravi Vatrapu, Dept. of IT Manage., Copenhagen Bus. Sch., Frederiksberg, Denmark, "e-Wallet Properties" on 17 October 2011 IEEE *Xplore*, Como, Italy.

[2] Zhimin Yang, Boying Zhang, Jiangpeng Dai, Dept. of Comput. Sci. & Eng., Ohio State Univ., Columbus, OH, USA, "E-SmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity, 2010 IEEE 30th International Conference.

[3] I. Kelenyi, J. K. Nurminen, Dept. of Autom. & Appl. Inf., Budapest Univ. of Technol. & Econ., Budapest, "Energy Aspects of Peer Cooperation Measurements with a Mobile DHT System" Communications Workshops, 2008. IEEE International Conference.

[4] Pinal Chauhan, J.H.Patel College of Management and Technology, Dahemi, “ E-Wallet: The Trusted Partner in our Pocket” Vol. 2, Issue 4, April 2013 (IJRMP)

[5] Basavaraj Nagesh Kadamudimatha, Lecturer in Commerce, S.G. Arts, Science and Commerce, College, Koppal, Karnataka, India, “ Digital Wallet: The next way of growth” Volume 2; Issue 12; December 2016; IJCMR

[6] RACHNA, Priyanga Singh,Assistant Professor in Commerce Shaheed Bhagat Singh College, University of Delhi (India) , “ Issues and Challenges of Electronic Payment Systems”, Vol. 2, Issue 9, December 2013 (IJRMP)

[7] Abhay Upadhayaya, Department of ABST,University of Rajasthan,Jaipur, India, “Electronic Commerce and E-wallet”, International Journal of Recent Research and Review, Vol. I, March 2012

[8] G.UDHAYARAJ and D. JOCIL, *Assistant Professor*, *Department of Commerce, Loyola College, Vettavalam, India, “*A study onElectronic Payment System” - “E-WALLET” International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) Volume 24 Issue 3 – FEBRUARY 2017

[9] Majid Taghiloo, Mohammad Ali Agheli , and Mohammad Reza Rezaeinezhad

[10] Amnafzar Department of Pishgaman Kavir Yazd, Tehran, Iran, “Mobile Based secure digital wallet for peer to peer payment system” International Journal of UbiComp (IJU), Vol.1, No.4, October 2010

[11] *Bogdan-Alexandru URS*, "Security issues and solutions in E-Paymentsystems”

[12] T. Vasudha Singh, N. Supriya, M. S. P. Joshna, Faculty, Department of Commerce, St. Ann's College for Women, Mehdipatnam, Hyderabad, Andhra Pradesh, India, “Issues and Challenges of Electronic Payment Systems”Vol5 Issue2, Jan2016, ijird

[13] Smita kakade, Jyoti kharade2,1Faculty, Dept. Of MCA, Bharati Vidyapeeth’s Institute of Management and Information Technology, India , “ Security in electronic transaction, Vol4 Issue4,Apr2017,irjet

.