

Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures

Mansi Bosamia^{1*}, Dharmendra Patel²

^{1,2}Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, CHARUSAT, Changa, Gujarat, India

*Corresponding Author: mansibosamia@gmail.com, Tel.: +91-94280-79200

Available online at: www.ijcseonline.org

Accepted: 19/Jan/2019, Published: 31/Jan/2019

Abstract— The volume of wallet payment transactions has considerably increased in the last decade. There are many wallets already has been developed and also new wallets coming in the market day by day for payment transactions in highly distributed environments. So far it has the focus on addressing only security issues. However, key important criteria of distributed processing such as performance, scalability, and availability. In this paper, we identify and analyze the different threats and vulnerabilities of a mobile cum web wallet application to obtain a high-level understanding of the various types of threats that may affect wallet applications with its possible security measures.

Keywords— e-cash, mobile payment system, mobile wallet












I. INTRODUCTION

About an earlier era, growing of e-commerce concerns has been expressed in the academic and financial communities about the future and safety. Now, the current era and recent future is of electronic cash, most common practice of e-cash payments is credit cards and debit cards. The recent trends of

payUmoney, hdfc zap pay, many more banking wallet apps, etc. Also, most of these are available as web wallet.

Mobile wallets have the key characteristics of physical cash such as anonymity, transferability, and security. Also they have few differences defines in table 1. The implementation and real-life deployment of mobile wallets schemes are inherently distributed with its processing issues including

Table 1. Comparison on different mobile wallets

Parameters	Apple pay	Google pay	Paytm	Freecharge	Mobikwik	SBI's buddy	ICICI pay	Airtel money	Jio money	payU money	HDFC zap pay
											
Year of launch	2014	2015	2010	2010	2009	2015	2013	2012	2015	2014	2015
Payment Type of wallet	Semi-closed	Semi-closed	Semi-closed	Semi-closed	Semi-closed	Semi-closed	Open	Semi-open	Open	Semi-closed	Semi-closed
Supports in-store proximity payment technologies	Yes (NFC)	Yes (NFC)	Yes (QR code)	Yes (QR code)	Yes (QR code)	Yes (NFC)	Yes (NFC)	No	No	No	Yes (QR code)
own UPI (Unified Payment Interface) based app	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes	Yes
Bank transfer	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes	No
Send on Mobile	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes
Company	Apple Inc.	Google	One97 Communications	Axis bank	One MobiKwik Systems Private Limited	State Bank of India	ICICI Bank	Airtel	Reliance	Naspers group	HDFC Bank
Industry	Technology	Technology	Private	Private	Private	Banking	Banking	Telecom	Telecom	Internet	Banking

e-cash is apple pay, Google pay, paytm, freecharge, mobikwik, sbi money, icici money, airtel money, jio money,

scalability, performance and availability. Till today, research on mobile payment has been directed mostly towards

addressing security requirements through the design of suitable security protocols and mechanisms. [6] For that, in this paper identifies the security threats. This paper defines mobile payment system which is similar to web wallet system, mobile wallet, mobile wallet threat model, and threats and vulnerability with wallets security measures. This paper organize as follows, Section I contain introduction and comparison of different mobile wallets, Section II contains mobile payment system working and Section III defines the various type of threats with its possible security measures. Section IV describes the conclusion and future scope of this paper.

II. MOBILE PAYMENT SYSTEM

Mobile payments have been popular and the most accepted as an emerging payment method in both advanced and emerging economies. Wallets are continues grow up and affects many factors such as increased deployments, mobile penetration, financial inclusion, more convenient, faster, and more economical.

A. Mobile Payment Definition

Mobile payment is payment services operated under financial guideline and performed financial transactions from or via a mobile device.

B. Mobile Wallet Definition

It is a virtual wallet in your Smartphone, in which money is stored in the form of virtual money. So overall, it is a digital wallet out of which you can make money transactions and payments. It has the combination of software and hardware on certain devices and all seek to replace the use of traditional credit/debit cards with mobile phones. You can pay money using smart phone apps, text messages, social media or websites.

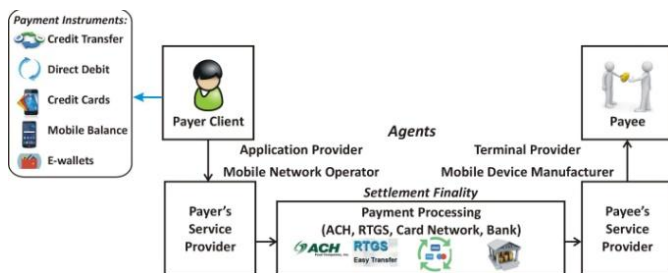


Figure 1. Mobile Payment System

In the mobile payment system, agents are playing main role. These agents are application providers, mobile network operators, mobile device manufacturers, terminal providers, and third-party agents. The client connects with mobile network using application provider. Application provider contains credit/debit cards details, mobile balance, bank account details for payment transaction. A mobile network operator provides services for make purchases, transfer

money, pay bills, etc. Other common services include third party payments, online services access, etc. Some mobile device manufacturers traditionally produce mobile phones with payment functions. Third party agents acting as retail outlets to deal directly with a customer for reducing services cost. Third party agents have sub-agents by the permission of law. Cash merchant agents provides cash-in and cash-out facility but not allows other banking transactions such as account open/close, loan, check, etc.

Currently, mobile wallets use has been increased due to more protected security aspects are enhanced. In past people don't have the acceptance of mobile base financial transactions but as the time changes, people has been accepted the payments solutions. Still there are many threats affecting to secure transactions to identify and understand the mobile wallets threat model in this paper.

III. MOBILE WALLETS THREAT MODEL

A threat model of mobile wallet applications such as paytm, apple pay, Google wallet, freecharge, mobikwik, sbi money, icici money, airtel money, jio money, payUmoney, hdfc zap pay etc. shall consider threats against basic components of the mobile wallet. Mobile wallets "trust boundaries" depicted below as dotted yellow lines. This area of mobile wallet has most possibilities for threats to occur. A generic threat model of the mobile wallet system is shown below: [7]

A. Mobile Wallet Application Users Threats

- *Phishing attacks:* Mobiles have personal and corporate information of customer which may to carry out sophisticated attacks. These attacks user by phishing emails. It is an attempt to trap a user to disclose the information.
- *Social engineering:* In social engineering, user data available in the public domain and the attackers can steal it from there. This information monetized or sold in underground market forums or used for fraudulent payments. Sometimes attackers use this theft information as their identity.
- *Unintentional installation of rogue and malware applications:* Attackers will install malware by malicious attachment, Redirecting the user to a malicious URL, insecure Wi-Fi hotspots, a network spoofing attack, fake access point with same network, fake website, etc. Then use user information for mobile wallet payment.
- *Mobile Operating System Access Permissions:* Users give certain permission to OS access, which can be use by attackers to access sensitive data and harm the mobile application.

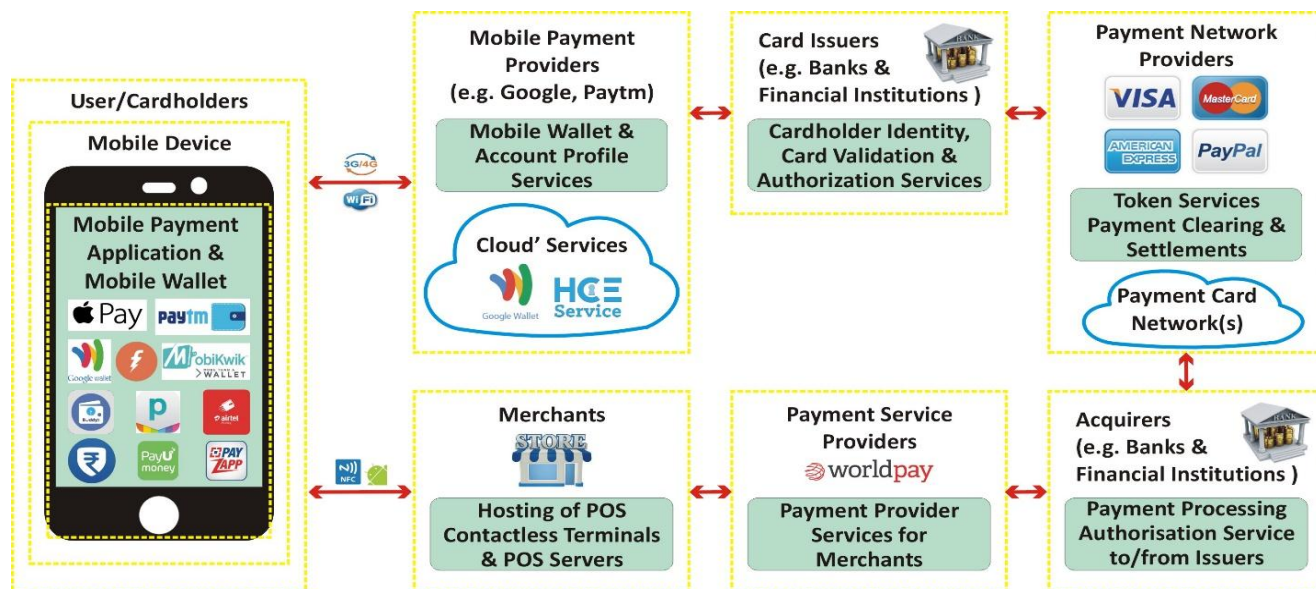


Figure 2. Mobile Payments and Digital Wallets Threat Model

The Possible Vulnerabilities of users are:

- Lack of user's due carefulness of validating content in emails, messages, SMS being truthful before selecting URLs, downloading attachments.
- Use public Wi-Fi connections for mobile payments.
- Use of fake access point with same network.
- Use of fake websites.
- Missing minimum security hygiene rules.
- To install non-trusted applications and files on device.

Possible Security Measures of Users

- Security awareness, education and communication.
- Do not use public Wi-Fi hotspots for mobile wallet payments.
- Distinguish real and fake website and access point, only use real one.
- Keep OS up to date and don't use entrusted phone.

B. Mobile Devices Threats

- *Unauthorized access of lost or stolen mobile device:* Once mobile has stolen then attacker can steal any sensitive data, also they have control on device. Attacker can also steal fingerprints data and used as provider authentication and use money of customer by fraudulent transactions. If the viruses and malware affected in stolen device then it is very real danger of lost or it affects consumer's digital live.
- *Data interception via installation of malware:* The installation of malware/root kits [11] can be allowed by drive by download attacks influence. For example, Web Kit to root level access, or by side-loading of malware alongside reliable or semi

reliable apps downloaded from the various stores.[7]

- *Mobile as a target:* Mobile devices are mostly targeted by attackers because once mobile is in their control they can use for any malicious attack like fraud transaction, use sensitive data, install spyware, etc. It is easy for attacker to attack on mobile device then mobile app.
- *Implementation Issues:* In a competitive market, all the payment providers are not going to stand still. It is predicted that new functionality will be continuously released. As such, there is a risk to run potentially immature code which may be prone to security issues on different implementation of mobile wallet payment application.

The Possible Vulnerabilities of mobile devices are:

- No PIN lock set or PINs set to weak PINs.
- No remote devices lock set and no remote data wipe set.
- Not up-to-date OS to connect and use entrusted device.

Possible Security Measures of Mobile Devices

- Remote device lock and Remote data wipe.
- PIN lock and Strong PINs.
- User to device biometrics authentication factors safely.
- Keep OS up to date.
- Keep default security controls & measures on device.
- Secured Biometric validation data.

C. Mobile Wallet Applications Threats

- *Reverse engineering:* Reverse engineering offers to attack on hardcoded passwords and encryption keys like data. For that attackers have high level of understanding of mobile wallet payment applications.
- *Tampering with the mobile payment application and the use of root kits:* An attacker may choose to backdoor a mobile payment application to capture login details and send these to an attacker controlled server. By this attacker can downloading and uploading any data from user application. This is a very realistic threat on mobile devices. [7]
- *Installation of root kits/malware:* Discussed in mobile device threats.
- *Mobile Operating System Access Permissions:* Discussed in mobile application user threats.

The Possible Vulnerabilities of Mobile Wallet Apps are:

- Hardcoded secrets as private keys.
- Missing to disable code debugging routines.
- Unsigned production binaries.
- Credit card provisioning weaknesses like stolen credit cards to affect sensitive data.
- Weaknesses in biometric identification for initial authorization of transactions.
- S/W vulnerabilities and weaknesses in third party applications that provide access to mobile wallets.
- Weaknesses in payment authorization provisioning with mobile paired smart watch device.
- Credit/debit card not stored encrypted in Secure Element or processed in Trusted Execution Environment.
- Weak PINs exposing them to brute force attacks.
- Insecure communication channels with Point of Sale (POS) contactless terminals.
- Insecure tokens used in Magnetic Secure Transmission (MST) connections.
- Poor signal strength for MST processing.

Possible Security Measures of Mobile Wallet Applications

- Adopt secure coding practices and secure code reviews manual and automated via tools.
- Source code complication entrusted code detection.
- Anti-debug and Integrity source code protections.
- White-box cryptography.
- Secure application provisioning through trusted application stores.
- Takedown rogue applications from unauthorized application stores.

D. Merchants Threats

- *Uploading malware (POS) on the POS contactless payment terminal:* Once the Point of Sale (POS) malware is installed on the POS contactless terminal it

can be configured by the attacker to remotely steal mobile wallet payment data that transact through the card readers. Uploading POS malware has insecure remote desktop access to POS servers. [7] It also affects the cryptogram and possibility of fraud payments.

- *Man-in-the-Middle (MiTM) attacks against the POS contactless terminal and POS server connections:* Attackers can also attempt to exploit network security weaknesses such as lack of firewalls.
- *Relay attacks against NFC enabled POS contactless terminal:* A known attack against the NFC POS interface is the relay attack. [7] Relay software installed on the mobile can relay commands and responses between the Secure Element and a card emulator that is installed as proxy on the mobile POS across a wireless network.

The Possible Vulnerabilities of Merchants are:

- Use of default password to access POS terminals available online.
- POS and POI security mis-configurations and security hygiene such as keeping software up to date, patching systems, etc.
- Insecure connections between POI and POS
- Insecure access to LAN and to POS systems
- Lack of enforcement of minimum privileges for POI and POS access

Possible Security Measures/Controls of Merchants

- Change default passwords on POS systems and keep POS software up to date.
- Use SSL between POS connection point (POI to POS).
- Deploy and configure firewalls.
- Restrict POI and POS access to authorized users.

E. Payment Service Providers Threats

- *Compromise of S/W running on contactless terminals:* Payment Service Providers (PSPs) provide POS contactless terminals for mobile payments e.g. for NFC enabled POS terminals as well as aggregated payment services for merchants by processing data from different channels including face to face (card present) payments, online payments and mobile/contactless payments.[7]
- *Compromise of Payment Gateways:* PSP payment gateways represent an interesting target for attackers that seek to compromise the payment data in transit from the merchants to the different acquiring banks.
- *Compromise of S/W installed on POS Servers:* Attackers might seek to compromise to attack on payment gateway and break the security of POS

contactless terminals that PSPs provide to merchants to host on their premise/network.

- *Data connectivity compromise:* Merchant hosted POS connection to Payment Service Provider (PSP) and from PSP to acquirer at that time Attackers might try to exploit insecure connections.

The possible Vulnerabilities Payment Service Providers are:

- Design flaws and un-patched S/W vulnerabilities in POI terminal/credit card machines and POS systems and payment gateways to/from acquirers.
- Insecure point to point connections between merchant POS server and PSP and between PSP and acquirers.

Possible Security Measures of Payment Service Provider

- Secure by-default design.
- Vulnerability testing
- Patching of POI terminal (card machines) H/W and S/W.
- Fix S/W vulnerabilities in POI.
- POI and payment gateways hosted at the payment service providers.
- Enforce secure point to point connections between merchant POS and PSP and between PSP and acquirers.

F. Acquirers Threats

- *Payment processing systems compromise:* When requesting token and cryptogram from the issuer payment network, attacker obtains large amount of cardholder data.
- *Installation of malware/RAT for Advanced Persistent Threats (APTs):* Attackers might seek to compromise the acquirer bank payment processing servers from the inside of the network. Installation of malware at backdoors and Remote Access Tools (RAT) via malware infection of the servers hosted at the acquired network.
- *Installation of root kits:* Root kits are a significant threat vector and can also be leveraged to directly monitor and hijack/manipulate API calls.
- *Data connectivity (external from acquirer to issuer and internal among servers) compromise:* Attackers might try to exploit insecure point to point connections between acquirer and issuer through network service provider network to conduct attacks.[7]
- *Repudiation of mobile payment authorization:* Repudiation attacks such as to repudiate a payment authorization from an issuer can be facilitated by exploits of design flaws in the implementation of payment processing services by the acquirers.[7]

The Possible Vulnerabilities Acquirers are:

- Un-authorized access to payment processing systems/applications and weaknesses in enforcement of internal security controls and measures to access these systems.
- Non-effective malware detection, data outflow detection/prevention and fraud detection/prevention.
- Insecure external and internal point to point system connections.
- Weak server to server authentication among internal systems.
- Gaps in non-repudiation controls for processing authorizations such as out of band verification/confirmation of suspicious transactions and digital signing of transactions.

Possible Security Measures of Acquirers

- Enforce high security standard measures for payment processing systems and second factor authentication (2FA) for user authentication/access.
- Enforce minimum privileges for user access.
- Deploy malware detection, data leakage and fraud prevention.
- Secure internal point to point connections with SSL/mutual authentication.
- Require digital signatures to sign and verify payment authorizations from issuer.

G. Payment Network Providers Threats

- *Compromise Token Services:* Tokenization services will become a single point of failure, something similar to DNS infrastructure. Token must be irredundant rather than like DNS. Additionally, they will become a prime target as they will map real PANs.
- *Compromise Token services provider servers:* Token Services Providers (TSP) provide token management services such as tokenization, de-tokenization and validation of the token data integrity and origination token and validation with cryptograms.
- *Denial of payment settlement services:* Attacks targeting the availability of token services hosted by payment network organization will impact the authorization of mobile payments and possibly also for payments originating from other channels that also use these token services.[7]
- *Data connectivity compromise:* Insecure connections to/from acquirers and issuers. Thus, the attacker may attack on this weak connection May stole the sensitive data.
- *Device and mobile network reliability:* the mobile device and network were considered unreliable for payments.

The Possible Vulnerabilities of Payment Network Provider are:

- Mis-configuration of servers providing tokenization services by Non-secure key storage.
- Insecure user access to the token vault.
- Insecure connections to/from acquirers and issuers.
- Weaknesses in protection of Denial of Service (DOS) attacks against TSP service.

Possible Security Measures of Payment Network Provider

- Secure configuration and hardening of critical servers.
- Secure key storage in hardware encrypted security modules.
- Dual controls and strong authentication 2FA to access the token vault.
- Enforcement of End to End encryption for protecting cardholder data in transit to issuer.
- Anti-DOS measures are application and network layer to protect token services.

H. Card Issuers Threats

- *Credit card Enrolment:* The first step to use a mobile payment is the enrolment of the user's credit cards into the app. The provider cannot concern about card holder or user. This is something that only the card issuer can know. Providers facilitate issuer's decision making by providing information to accept or not.
- *Payment authorization process compromise:* An internal attacker at the card issuer bank or an external attacker that gained access to critical servers may attempt to bypass fraud controls e.g. changing the card payment limits.
- *Confidential cardholder data compromise through malware/APT:* Credit and debit accounts mostly target for commit fraud or reselling accounts information in black market. It can attack user's sensitive data to attack in banks databases. Possible attacks are first, using social engineering authenticate bank and access databases, and second, Advanced Persistent Threats (APTs) that seek to install malware to target encryption keys or supplementary data.
- *Payment fraud:* Payment fraud detection should occur at fraudulent mobile payments transactions, enforce credit card limits on the payment transactions themselves and on the debit cards amounts linked to consumer direct bank accounts managed by the issuer bank.
- *Token services data compromise:* Issuers can choose to leverage the tokenization service from the payment networks or implement their own token service and become a Token Service Provider themselves; they will be at increased risk of threats against token data confidentiality, integrity and availability.

The Possible Vulnerabilities of Card Issuer are:

- Weaknesses in enforcing strong authentication for access to critical systems and databases where cardholder data is stored for validation and payment authorization to acquirer.
- Non-effective malware detection and prevention measures.
- Misconfiguration of fraud detection systems including rules such as positive payment checks, max limit amount per transaction, daily limits, velocity tagging.

Possible Security Measures of Card Issuer

- Enforce strong multi-factor authentication for access to critical systems where credit cardholder data is being stored.
- Enforce minimum privileges for users that have access to internal critical systems used for verify cardholder data and authorize payments based upon specific business rules.
- Deploy malware detection and prevention, suspicious activity detection rules based upon aggregated log analysis.
- Configure fraud detection and prevention systems and enforce fraud management rules for mobile payment transactions.

I. Mobile Payment Applications Providers (Servers & Cloud Services) Threats

- *Compromise of cardholder's sensitive data:* Attackers might direct their effort to cardholder credit/debit data and personal data of the user that is stored by the mobile payment service provider. [7] This data compromise might also occur during transmission at the time of card enrolment.
- *Compromise of the user profile managed in the cloud:* Since the mobile application has access to the mobile payment servers. At the time of card enrolment an attacker could enrol stolen credit data with the mobile card enrolment service, to abuse non-authorized access to the user profile managed at the mobile payment provider, and to change accounts sensitive data to facilitate fraud.[7]
- *Token service data compromise:* Since mobile payment providers can also implement their own token service they are also at risk of threats against the token management process that encrypt and decrypt tokens, the management of keys and the integrity and availability of the tokens issued for payment authorizations. [7]
- *DDoS attacks:* DDoS attacks by threat actors seeking to interrupt mobile payment services. These might affect transactions relates services hosted in the cloud.

- *Enrolment of stolen credit card data entry:* Enrolment of stolen credit card data for use of mobile payment by fraudsters. Attacker uses the phone's camera, memory scraping, OCR recognition, etc. information and sent on cloud to gain access the network traffic of user's data. The attacker could masquerade passbook and steal card information.
- *Accountability for payment transactions:* Payment providers require fingerprint authentication to perform the payment. As individual by figure print and more than one device access creates accountability identification failure in mobile payments.
- *Transaction errors:* The errors could be caused by the payment system or by their own mistakes in the system use.
- *Lack of transaction record and documentation:* It difficult to follow up the amount of payments made with a mobile phone since they did not get any receipt or other efficient means to keep track of the payments.
- *Ambiguity of the transaction:* The lack of control when paying with a mobile phone. They were unsure of whether the payment had taken place or not and whether the payment had been charged or not.
- *Third party trust:* Regardless of the mobile payment provider, enrolling on the system requires a certain level of trust on the third party.
- *Privacy issues:* some of the respondents were unwilling to trust their personal information with the payment service providers. They were concerned that their purchases would be tracked or that they would begin to receive a lot of advertisements.

The Possible Vulnerabilities Mobile Payment Application Providers are:

- Weaknesses and vulnerabilities on digital wallet servers and applications hosted at the mobile payment application provider.
- Absence of malware detection and prevention on critical servers that provide access servers where cardholder data and user profiles are stored.
- Gaps in deployment of 2FA to access servers and maker/checker controls.
- Absence of fraud detection and prevention for use of stolen credit card holder for enrolment in mobile payment applications.
- Weaknesses in anti-DoS measures to prevent DoS against digital wallet and account profile services hosted in data centers and cloud services.

Possible Security Measures of Mobile Payment Application Provider

- Enforce information security policies and processes requiring identification and remediation of vulnerabilities in servers and applications.

- Deploy malware detection and prevention measures.
- Enforce 2FA for internal user's access to critical servers such as digital wallet services where cardholder data and user profile information is stored.
- Enforce user entitlements and minimum privileges.
- Deploy fraud detection and prevention for high risk functions such as change of account profile, credit card enrolment and payment transactions.
- Deploy anti-DoS measures for critical servers hosted in data centers and in the cloud.

IV. CONCLUSION AND FUTURE SCOPE

There are many potential wallet threats and vulnerabilities are identified. However, the threats are identified yet not reached to the expected level of maturity; as a result the overall field proceeds to be an area of intense research. Due to fast development of wallets most of solutions are already implemented. Also need to identify new solutions for specific threats or vulnerability. This paper also indicates that if the new solution is identified then defiantly increase the "trust boundaries" of wallet payments.

REFERENCES

- [1] Dahlberg, Tomi, Niina Mallat, and Anssi Öörni. "Trust enhanced technology acceptance model-consumer acceptance of mobile payment solutions: Tentative evidence." Stockholm Mobility Roundtable 22 (2003): 23.
- [2] Hoofnagle, Chris Jay, Jennifer M. Urban, and Su Li. "Mobile payments: Consumer benefits & new privacy concerns." (2012).
- [3] Kasiyanto, Safari. "Security Issues of New Innovative Payments and Their Regulatory Challenges." In Bitcoin and Mobile Payments, pp. 145-179. Palgrave Macmillan UK, 2016.
- [4] Khiaonarong, Tanai. "Oversight issues in mobile payments.", IMF Working Paper (July 2014).
- [5] Hohl, Fritz. "Time limited blackbox security: Protecting mobile agents from malicious hosts." Mobile agents and security (1998): 92-113.
- [6] Simplot-Ryl, Isabelle, Issa Traoré, and Patricia Everaere. "Distributed architectures for electronic cash schemes: a survey 1." International Journal of Parallel, Emergent and Distributed Systems 24, no. 3 (2009): 243-271.
- [7] Security of Mobile Payments and Digital Wallets, ENISA December 2016, https://www.enisa.europa.eu/publications/mobile-payments-security/at_download/fullReport
- [8] Allen, Hellen, 2003, "Innovations in Retail Payments: E-Payments", Bank of England Quarterly Bulletin, Winter, pp. 428-438.
- [9] Diniz, Eduardo Henrique, João Porto de Albuquerque, and Adrian Kemmer Cernev. "Mobile Money and Payment: a literature review based on academic and practitioner-oriented publications (2001-2011)." (2011).
- [10] Urban, Jennifer. 2016. "Mobile Payments: Consumer Benefits & New Privacy Concerns". SocArXiv. July 18. osf.io/preprints/socarxiv/7pnxz.
- [11] Papathanasiou, Christian, and Nicholas J. Percoco. "This is not the droid you're looking for..." Def Con 18 (2010).
- [12] Davis, Michael, Sean Bodmer, and Aaron LeMasters. Hacking Exposed Malware and Rootkits. McGraw-Hill, Inc., New York, NY, USA, 2009.
- [13] The Great Bank Robbery: Carbanak APT <https://business.kaspersky.com/the-great-bank-robbery-carbanak-apt/3598/>

- [14] FIDO Alliance, "Specifications Overview", <http://fidoalliance.org/specifications/overview/>
- [15] https://en.wikipedia.org/wiki/Mobile_payment
- [16] European Central Bank, "Recommendations For The Security of Mobile Payments", <https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf>
- [17] ENISA, "Mobile Identity Management", <https://www.enisa.europa.eu/publications/Mobile%20IDM>
- [18] Drop Labs, "Rampant: Explaining the Current State of Apple Pay Fraud", <http://www.droplabs.co/?p=1231>
- [19] Apple, "About EMV and Apple Pay for Merchants", <https://support.apple.com/en-us/HT205645>
- [20] ISACA, "2015 Mobile Payment Security Study", <https://www.isaca.org/Pages/mobile-payment-security-study.aspx>
- [21] Mobile Payment in Your Business", <https://www.intelligentq.com/resources/the-3-biggest-benefits-of-implementing-mobile-payment-in-your-business/>
- [22] Salvador Mendoza, "Samsung Pay: Tokenized Numbers, Flaws and Issues", <https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues-wp.pdf>
- [23] Zvelo, "Google Wallet Security: PIN Exposure Vulnerability", <https://zvelo.com/google-wallet-security-pin-exposure-vulnerability/>
- [24] Wonder How To, "Apple Watch Vulnerability Lets Thieves Use Apple Pay Without Your PIN", <http://ios.wonderhowto.com/how-to/apple-watch-vulnerability-lets-thieves-use-apple-pay-without-your-pin-0161940/>
- [25] <http://viaforensics.com/mobile-security/forensics-security-analysis-google-wallet.html>
- [26] MIT Technology Review, "Is Google Wallet Safe ?", <https://www.technologyreview.com/s/426921/is-google-wallet-safe/>
- [27] Choi, Daeseon, and Younho Lee. "Eavesdropping One-Time Tokens Over Magnetic Secure Transmission in Samsung Pay." In WOOT. 2016.
- [28] Trend Micro Discovers MalumPoS; Malware Targeting Hotels and other US Industries <http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-malumpo-s-targets-hotels-and-other-us-industries/>
- [29] <https://www.goodreturns.in/classroom/2016/11/types-mobile-wallets-their-difference-518655.html>
- [30] <http://www.dqindia.com/top-6-mobile-wallets-in-india/2/>
- [31] <http://www.iamwire.com/2016/11/list-of-mobile-wallets-upi-payment-apps-in-india/145172>

Authors Profile

Mansi P. Bosamia, B.C.A., M.C.A. and Pursuing Ph.D. at Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science and Technology, Changa, Anand, India. She has more than 5 years teaching experience and 3 years Research experience. She has published/presented 7 papers in national/international conferences/journals of repute. She wrote two books related Data Structures and Algorithms. Her areas of interest are Computer Algorithms, Data Structures, Networking, Computer Graphics, Mobile Computing, Cryptography, etc.



Dr. Dharmendra Patel, B Sc.(I/C), MCA, SET, Ph.D. (Computer Science). He is working as Associate Professor at Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science and Technology, Changa, Anand, India. He has published/ presented 15 research papers in national/ international journals/conferences of repute. Also, served as editorial/review board members in many international journals and have reviewed 25 papers of different international journals of repute. His areas of interest are Web Mining, Distributed Operating Systems, Cloud Computing, Soft Computing, Software Engineering, Data Structures, and Mobile Computing.

