International Journal of Engineering, Science and Mathematics
Vol. 7 Issue 9, September 2018,
ISSN: 2320-0294 Impact Factor: 6.238
Journal Homepage: http://www.ijesm.co.in, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Security in Next Generation Mobile Payment Systems:1

[1]Vikas chaudhary, [2] Sandeep Mittal
[1,2]Department of Computer Science and Engineering, RD Engineering College
Ghaziabad (U.P), India-201206

Corresponding author- vikaschaudhary@gmail.com

ABSTRACT:

Mobile payment is the killer application in mobile commerce. We classify the payment methods according to several standards, analyze and point out the merits and drawbacks of each method. As a kind of mobile data service, mobile payment service has approached people's lives. It main focus on field of telecom service provider. Before the mobile payment system Radio Frequency Identification (RFID) is transaction solution [4].

Cash payment is still king in several markets, accounting for more than 90% of the payment s in almost all the undergoing growth countries. The use of things not fixed telephones is good looking normal in this present time. Readily moved telephones have become a together the entire time friend for many users, giving out to much more than just news apparatus for making or put right things. Every coming after person is heavily being dependent on them because of, in relation to much-sided use and payment power.

We explore multiple proposed models of the mobile payment system (MPS), their technologies and comparisons, payment methods, different security mechanisms involved in MPS, and provide analysis of the encryption technologies, authentication methods, and firewall in MPS. We also identify current challenges and future directions of mobile phone security.

Smartphone instead of cash:-

Mobile phones companies, network operators and financial institution promise themselves to make phones capable for money exchange. As per a study expansion of mobile devices in upcoming years will increase significantly. Through this paper we will discuss how software system handles the payment process by the usage of mobile devices and the payment servers.

Wireless communication is making a big impact to daily life. The swift advance of wireless networking, communication, and mobile technology is make huge impact. The significant increase of mobile device users in the recent years causes a strong demand on secured wireless network and reliable mobile commerce application. Since mobile is critical part of most wireless information services and application.

1. INTRODUCTION:

Mobile commerce is defined as any transaction with a monetary value that is conducted via a mobile telecommunication network. Cash payment is still ruler in several markets, accounting for more than 90% of the payments in all almost all the developing countries. In our time, the use of readily moved apparatuses by people has increased greatly[1]. A much number of people use things not fixed telephones to act day-to-day task. These apparatuses can be used for many works, such as making telephones cries, web surfing, emailing, playing activity, and many other works.

Simplified the current operation of making observations in this area is gave all attention on the use of things not fixed telephones to act payment safely. However, things not fixed systems face several limiting conditions such as low place for storing and computation powers, because of, in relation to which they cannot act weighty process of changing

knowledge into a secret from operations. Different attacks are stated on readily moved apparatuses because of, in relation to existence without of safety bits of

land such as spoofing, phishing 3, malware 4, and smelling attacks.
The advancement of wireless networking and communication, and mobile technology is changing people's life. As there is a significant increase of mobile device users, mobile payment method are needed more wireless services. The system is two dimensional secured protocol to support the peer to peer transaction between two mobile clients.
This m-payment system can be used in different scenarios such as:-

- M-payments between a passenger and taxi driver.
- M-payments between merchants in flee market and their customers.
- M-payments for parking fees and subways.

The purpose of this paper is to make a software for manage the payment process through the use of mobile device and a decentralize payment server. This payment server is work as a gateway between the mobile device and the bank server.
In recent years, RFID has been used in logistic information system by the promoting many organization such as Wal-mart, Gillette, P&G etc. that RFID has focused on global industries and been one of the most promising industry this country [4]. The unique function of RFID tech is it could identifying anyone and anything in real life by the tech in virtual reality network because of its function-Tagging , addressing, sensing.

1) ACCOUNT BASED PAYMENT SYSTEM

In account-based transactions, we need cards or information cards like ATMs or credit cards. Using this process, the user's Bank account charges the amount after getting the required details or confirmation of the user's transaction. Risk Factor: If any misuse of a card or details is done or any forgery or identity theft is done, then it will affect this system.

2) TOKEN BASED PAYMENT SYSTEM

It is a new electronic payment method based on tokens instead of cash or credit cards. These tokens are generated by any bank, service provider, or telecom company. Moreover, it is used in the same way as cash is used. By using such tokens, users can pay to any company through mobile, and those tokens will be sent to that company which they can encash , or the provider will pay them for each token. Risk Factor: These tokens will have no worth if the user has tokens in their account and the merchant does not accept those tokens.

2. RELATED WORK:

In all the developing countries cash payment accounts for more than 90% of the payments. So, is necessary to realize the importance of Mobile Payment acceptance. Generally studies on MP implementation have focused on the user side, considered the user behavior on the MP is significant to advance MP services to improve users acceptance intention. The author is tried to present different types of online payments such as credit card, debit card , e – wallet , net banking , smart card , mobile payment , and Amazon pay. The author used cryptography technique for the authentication between server and client.
In today world most of online payment transaction is done through UPI in India. For the international transaction the communication between the payment server and

corresponding bank server through SWIFT electronic bank communication. This standard can also be used for automatic realization of a payment process that means realizing the payment without user interaction on the payment server side while using the secure technique of standard.

A-Mobile payment system (MPS) boost in developing countries:-

1. SOCIOECONOMIC CONDITIONS
2. COST EFFICIENCY
3. DIFFUSION OF MOBILE PHONES
4. CONVENIENCE

B-FACTORS LIMITIN MP DEVELOPMENT

1. HEAVY REGULATION
2. LIMITED COLLABORATION
3. UNDERDEVELOPED ECOSYSTEM
4. SECURITY PROBLEMS

MOBILE PAYMENT SYSTEM SECURITY MECHANISM:-

MPS security mechanism includes: Encryption technology, authentication, and a firewall.

3. AUTHENTICATION METHOD IN MPS:

This method is used to test user identity in mobile transaction as the user identity is required to execute transaction. Authentication is different types such as – 1. Knowledge based authentication verification, 2. Object based authentication and 3. Biometric based authentication. There are three types of authentication factors- Single factor authentication (SFA), two-factor authentication (2FA), multi-factor authentication (MFA).

As mention earlier the identification of the devices should be handled in an abstract way. Through software design the system should be able to provide a variety of specific procedures for unique identification. The first type is known as account-based payment systems, in which each customer is associated with a specific account maintained by a trusted third party.

The second types of wireless payment is mobile POS payment systems that allow customers to purchase goods on vending machine or at the retail store with their devices. This payment method is designed to complement existing credit and debit card system for mobile users.

Authentication procedure occur when two mobile devices communicate with each other for the first time. Before operating any payment process both the parties payer and receiver should have logged in payment system.

4. CYBERATTACKS ON MOBILE PAYMENT SYSTEM:

Multiple types of attacks on MPS can come from unauthorized malicious users. The first attack is targeted on user PIN via surfing when it is unmasked PIN of four to five digits. The second type of attack occurs on money communication channels where hacking is possible. The third types of attack are at the server of the mobile money app.

A mobile payment system was targeted in a devastating cyber attack, causing widespread disruption and financial loss. Hackers exploited a vulnerability in the system's security protocols, gaining unauthorized access to sensitive user information, including payment card details and personal data. The attack resulted in fraudulent transactions, leading to financial losses for both the mobile payment system provider and its users. The system was temporarily shut down to contain the breach and investigate the extent of the damage. The

incident raised concerns about the security of mobile payment systems and the need for robust cyber security measures to safeguard against such attacks in the future. Users were urged to change their passwords and monitor their accounts for any suspicious activity. The incident served as a stark reminder of the escalating threat of cyber attacks on mobile payment systems and the critical importance of protecting user data from malicious actors.

5. SECURITY ANALYSIS OF M-PAYMENT SYSTEM:-

Mobile payment systems require robust security measures to safeguard against cyber attacks, protecting user data, payment card details, and preventing fraudulent transactions. Regular security audits, encryption, authentication protocols, and user education are critical to ensure the integrity, confidentiality, and availability of the system and instill user confidence.

This system presents the security analysis of the M-Payments system. Security analysis is collection of various services- authentication, mutual authentication, integrity, customer anonymity and non-repudiation.

The basic security solution of the P2P-Paid payment system is an integration of the secured payment protocol, biometric verification, and optimized security methods. Each element in the security header can be empty or contain values that depends upon what types of information is sent. The basic format of security header is:

Mac - key used - key length - encrypted field

The basic security system solution of the payment system is Bluetooth environment provide the following features. Such as –

a) Account Service:-

Before using the online payment service in Bluetooth environment, a user must have an account in bank.

b) Access Control:-

Authorization comes after authentication. In order to use the payment service, a user has to login first. Only the authorized user receives the access to the system. Mobile payment system require the user to enter the account number and PIN number over the mobile devices.

c) Security Verification:-

In mobile payment system a user need to fill valid account number and password at system. Payment server checks the information about account number and password in database and the process list otherwise the account number and password mismatch and error information.

6. CONCLUSION:

This paper discusses about multiple payment schemes and their usage, technology, and provided security mechanism. We present an overview and discussed different components of MPS. We include different aspects of MPS, including socioeconomic conditions, cost efficiency, diffusion of mobile phones, convenience, underdeveloped ecosystem, and security problems.

The wireless payment system is not only support mobile payment transaction over a wireless internet, but also support wireless payment transaction between two mobile phones over a network [3]. We also discuss analysis of encryption technologies, authentication methods, and firewalls in MPS. All the papers suggest different techniques to provide different security aspects. Therefore the main point is that keeping in check each payment should be made with authentication and encryption because the future of MPS depends on its security features. The aim of this paper is to make a software system for manage the payment process through the usage of a mobile device and a payment server.

Our mobile payment system takes usability, cost and security, extensibility into account, and now is operating in "Settlement Network for Mobile Commerce" [6].

It's clear that payment vendors will improve their solutions on continue basis to keep up with the changing technological aspect. Successful payment methods will be those that can continue to meet the many requirements mentioned in this paper, such as - cost, technical requirement, particularly security. In conclusion, securing mobile payment systems is essential to prevent cyber attacks, protect user data, and maintain trust. Robust security measures, regular audits, encryption, authentication, and user education are vital for ensuring system integrity and safeguarding against potential breaches.

REFERENCES:

[1] Bundesverbandes deutscher Banken e.V. (2006) FinTS-Spezifikation Version 3.0. [Online] . Available: http://www.hbci-zka.de/spec/3 0.html

[2] G.Lawton, "Moving JAVA into mobile phones," IEEE Computer, vol. 35, no. 6, pp 17–20, 2002.

[3] H.M. Yunos, J Gao, and S. Shim, "Wireless Advertising's Challenges and Opportunities: IEEE Computer", Vol. 36, No. 5

[4] Bhuptani Manish, Moradpour Shahram, "4RFID Field Guide: Deploying Radio Frequency Identification systems", Prentice Hall PTR

[5] N.M. Sadeh, M-Commerce: Technologies, Services, and Business Models, Wiley, John & Sons, Inc., March 2002

[6] Durlacher, "Mobile Commerce Report", technical report of Durlacher Research Ltd, 1999.