Introduction

An Architecture for Secure Mobile Payment System using Public Key Infrastructure
Chapter I

INTRODUCTION

Mobile Commerce is an emerging discipline that involves mobile devices, applications, middleware and mobile networks. Mobile Commerce is considered as a natural successor to e-commerce. Compared with traditional e-commerce, mobile commerce can really make anyone gain the entire information and services at any time, any place and on any device. There has been in these days a notable increase in consumer use of mobile applications. Mobile phones are well suited for mobile commerce to reach the customers through messages. In this scenario, m-commerce applications have been facilitated by Automatic Teller Machines (ATMs), banking networks, electronic bill payment systems and several such applications.

The rapid growth of wireless networks and services fueled by next generation mobile communications systems research has ushered in the area of ubiquitous computing. Light weight portable computers, IP based office and home appliances, and the popularity of Internet are strong forces to the service providers to support seamless user mobility. Realizing commercially viable secure IP mobility support over the current cellular infrastructure remains a research challenge.

Over the last few years, a number of mobile communication systems have been developed and numerous service providers and equipment vendors are bringing to market a steady stream of new innovations. The Wireless and mobile communication infrastructure could be used as a good platform for the growth of
mobile commerce applications with the multi-functionality mobile devices. The other key drivers for the evolution of m-commerce are ease-of-use, convenience, and anytime-anywhere availability. Additionally, Mobile commerce facilitates day-to-day activities such as entertainment, messaging, advertising, marketing, shopping, information acquisition, ticket purchasing, payment, mobile banking and others. Underneath the hype and publicity over these new technologies, the design specifications and the physical properties define the capabilities and limitations for mobile communications networks and its applications.

1.1 The Mobile Devices Penetration

Mobile devices have been the fastest adopted consumer products of all time compared to Personal Computers. The proliferation of mobile devices has been a truly unexpected opportunity for communication by supporting the advantages of mobility. In terms of sheer number, mobile phones at the end of 2003 were 1.4 billion serving about 25% of the world’s population, whereas there were only 607 million Personal Computers (PCs) including desktops and laptops and a negligible small number of Personal Digital Assistants (PDAs). Worldwide mobile phone penetration rate has exceeded 60% and it is estimated that it would reach 75% in 2011 [Wansink 2009]. The number of mobile subscribers in India has crossed 653.92 million in June, 2010 and grew six percent from May, 2010 with an addition of 36.39 million new connections. According to data released by the Telecom Regulatory Authority of India (TRAI), the wireless user base grew 2.7 percent to 617.53 million in May, 2010 from 601.22 million in April, 2010 [The Economic Times 2010].
Today, India and China are the dominant players in mobile communication field. According to China’s Ministry of Industry and Information Technology (MIIT), the subscriber base of China grew to 702.65 million in July 2009 [Wireless Federation 2009]. Frost and Sullivan estimated that world-wide mobile penetration was 42% in 2008 and it would reach 53% penetration by 2014 worldwide [Ortiz 2008]. Figure 1.1 presents the worldwide mobile and mobile subscriber penetration.

**Figure 1.1:** World-wide Mobile and Mobile Subscriber Penetration

The graph represents that the mobile phones are used by billions of people and continue to maintain a lead because of a rapid rise in the number of subscribers belonging to countries like China, India and Russia. With the increasing numbers of mobile users, the mobile phones gradually become a computing device for many applications and in near future the differences in communication and computing may exist as a single intelligent mobile device.
1.2 Mobile Payments

Mobile Payment is a natural evolution of e-payment scheme that will facilitate mobile commerce. Any payment where a mobile device is used in order to initiate, activate, and/or confirm this payment can be considered a mobile payment [Au et al. 2008]. Mobile devices such as mobile phones, PDAs, wireless tablets connect to mobile telecommunication network and make it possible for payments [Karnouskos et al. 2004]. Mobile phones are becoming an increasingly popular mode to make all categories of payments. Mobile payment will empower the existing m-commerce applications facilitating the transactions for general or particular services. The long term goal of mobile payment system framework in India would be to enable funds transfer from account in one bank to any other account in the same or any other bank on a real time basis irrespective of mobile network a customer has subscribed to. This would require interoperability between mobile payments service providers and banks and development of a host of message formats.

The mobile payment is carried out with a mobile payment instrument such as mobile credit card or a mobile wallet. The payments are also possible with point-of-sale terminals. The mobile payment ecosystems involve different stakeholders such as Mobile Network Operator (MNO)-centric, bank-centric, vendor-centric, technology centric, etc. It also provides different models like Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Consumer (C2C) and, one-way and two-way Person-to-Person (P2P).
Mobile payments are still being used primarily by people in all walks of life [McPherson 2004]. Figure 1.2 presents the various stages of mobile payments evolution.

![Figure 1.2: Stages of Mobile Payments Evolution](image)

Mobile payments expand more quickly on location-based services such as traffic reports and driving directions are available that are clearly superior to substitutes in the wired world. When mobile payments are used, the merchants see an opportunity in supporting them with unique technologies. However, the mobile payment services have not reached maturity due to lack of security at different levels.

The growth of mobile payment market in India increases rapidly. People in India are utilizing their mobile phones for purchasing goods, banking services, and for money transfer on daily basis. The Indian Mobile payment Market forecast is that

---

*An Architecture for Secure Mobile Payment System using Public Key Infrastructure*
the gross transaction value of mobile payments will reach $1.28 billion by 2013 [Wireless Market Research 2009].

The mobile payment user penetration in Asia Pacific and Japan is predicted to increase two percent in 2009 to 3.8 percent in 2012. In Western Europe, the mobile payment user penetration is expected to rise from 0.9 percent in 2009 to 2.5 percent in 2012. In Eastern Europe, the Middle East, Africa and Latin America, it is expected to cross three percent in 2012 [Gartner 2009]. The world-wide mobile payment user penetration is depicted in Figure 1.3.

![Mobile Payment user Penetration in 2010](image)

**Figure 1.3:** World-wide Mobile Payment User Penetration

Since the Indian mobile phone subscriptions are growing to the tune of 17.9 million a month, payments professionals are optimistic about the developments of mobile payment systems, but expect that it will take time for the industry to mature and develop. A survey has been conducted by Mobile Payment World Magazine in India. Individuals were invited to participate in the survey via email and 89% of
people voted that mobile payment solutions will soon rapidly grow in India [Mobile Payment World 2008].

1.3 Mobile Payments Services

Mobile payments have attracted many researchers globally. Several mobile payment services as well as access to electronic payment and Internet banking have been introduced all over the world, but each one has its own limitation. Several mobile payment service initiatives in European Union (EU) countries listed in the ePSO database in 2002 have not reached the target [Dahlberg et al. 2007]. In Europe, the development of mobile payments has not been successful, with the exception of several countries such as Austria, Spain, Croatia and the Scandinavian countries. However, Asia Pacific countries have attained a level in utilizing the mobile payment services. The main difference between successful implementations of mobile payment services in the Asia Pacific region and failure in Europe is primarily attributed to the ‘payment culture’ of the consumers that are country-specific [Carr 2007].

In Asian countries like Japan, South Korea, and Malaysia, several successful mobile payment solutions have already been launched namely Mobile Suica, Edy, Moneta, Octopus. NTT DoCoMo is also quite successful with the launch of the “osaifu-keitai” wallet service. The 20 million subscribers have been equipped with this payment service within a year and 1.5 million subscribers have already activated the credit card functionality. There are about 100,000 readers installed in Japan and it is expected to register an increase exceeding 150,000 readers [Ondrus et al. 2007].
Mobipay is a mobile payment mechanism that allows customers to pay for goods through their mobile phone. It works currently in Spain, and is expected to be introduced in other countries in the near future. Mobipay works for both virtual and real POS payments [Hassinen et al. 2006].

In the United States (US), financial institutions like banks, card companies, payment service providers are also working on mobile payments. Visa, MasterCard and American Express already proposed a version of their credit card with an RFID chip to enable contactless payments. However, in terms of phone-based systems, the mobile payment market is rather immature in US. At Atlanta's Philips Arena, Visa is exploring the potential of mobile payment technology using Near Field Communication (NFC) [Ondrus et al. 2007].

India and China are the two largest giants in mobile market. The mobile penetration level in China is far higher than in India. Despite the high level penetration, the new products and initiatives of mobile payments in China are often rolled out. The key players such as China UnionPay, China Mobile and national level players are focusing specific payments such as SmaartPay, Yeepay, Alipay, China Paypal, paipai, QQ, China M-World. In India, mobile payments like mCheck, Obopay and Paymate are providing a platform for the development of new payments [KPMG 2007].

Of late, efforts are on to promote the growth of the mobile payment services. The World Wide Web companies are planned to introduce m-payment services. Due to the economic constraints and the decrease in willingness to finance high-risk technology-based activities, many of them have stopped to exist or have frozen their
activities. However, the current state of mobile payment systems and services are listed in [Karnouskos et al. 2004].

1.4 Mobile Payments and Its Security Limitations

The most important issue related to the mobile payment systems and services is security. Nowadays, several systems are in use offering mobile payment transactions. However, the current security solutions adopted in mobile payment environments at the communication layer are not adequate [Feng Zhang 2010]. Security at the application layer must be added in order to achieve end-to-end protection for mobile payment environments. The security challenges in mobile payment are related to but not limited to the mobile devices, the radio interface, the network operator infrastructure and the type of transaction. Therefore, the development of secure mobile payment system has become a major research topic in the field of mobile commerce for the research community and telecommunication industry.

The basic security services for mobile payment environments are authentication, confidentiality, data integrity and non-repudiation. The existing payment systems have adopted symmetric and asymmetric cryptographic operations to achieve high level security. Although the mobile devices need more power consumption to perform public key operations, the protocol designers in recent years are providing lightweight security mechanisms using Public Key Infrastructure (PKI). The PKI is a system of digital certificates, certification authorities, and other registration authorities that provides solutions to enable secure mobile payment transactions.
There are number of issues limiting the security in mobile payment environments [Josang et al. 2003]. The major problems in successful payments are lack of adequate security. The encryption techniques such as secret-key and public key infrastructure are the most common methods to ensure transaction privacy, confidentiality and integrity. However, these techniques are depending upon the security of the endpoint systems in terms of protecting the keys from modification or misuse [Marchany et al. 2002]. The public key encryption techniques are the standard mechanism to adopt security like network security, operating system security, application data security and Digital Rights Management [Tiwari et al. 2007].

The threats posed to payment application servers fall into two categories: threats from an actual attacker and threats accruing from technological failures. The direct threats to payment servers are Malicious Code threats that include viruses, Trojan Horses, Logic Bombs, transmission threats such as Denial of Service (DoS) attacks, Ping of Death Attack, and SYN Flooding. The other threats to payment servers are Data Packet Sniffing, IP Spoofing, and Port Scanning. The network security threats are classified further into interruption, interception, modification, and fabrication which also are in the design and development of mobile payment system [Jung et al. 2001].

The limitations listed above are of the mobile payment transaction systems. Therefore, a novel, effective, lightweight and flexible security solution is needed for mobile payment transaction environments.
1.5 Aim and Objectives of this Research

The aim of this research is to propose an architecture for Secure Mobile Payment System using Public Key Infrastructure. The Mobile Payment services have become very essential for every human being at their personal level and professional level. The research reveals that different approaches came to the market for secure mobile payment system to address the existing needs of common man, but a global solution does not exist so far due to the regulatory barriers, lack of interoperability with banks and other operators, service complexity and bad user experience, and poor interest from consumers [Andreoli 2008]. In particular, there is no global mobile payment system for educational institutions to collect the fees as well as for student community to pay the fees through their mobile hand held devices. The large number of higher academic institutions all over the world, the traditional and present practices of payment of fees are cumbersome and time consuming.

The existing payments systems and solutions are unsuitable for payments related to academic side. In general, different players such as consumers, content providers or merchants, Payment Service Providers (PSP) and the Trust Third Party (TTP) are performing the unique roles in mobile payment process. The consumer is the person owning the mobile device and is willing to use it to pay for a service or product. The mobile user’s roles may involve initializing the mobile purchase, registering with the PSP and authorizing the payment.

In academic institution related payments, the beneficiary (payee) is the educational institution and it does not deliver any goods or products as return. In order to make use of payment service, the consumer must create a separate account with MNOs or
with independent PSP like PayPal [Hassinen et al. 2005]. Some of the payment service providers ask their customers to deposit the amount onto their accounts. If the client maintains an insufficient or less amount, he can not avail the payment service. Otherwise, the service providers may provide extra charges for delay payment made by the client in credit card payment systems. However, these procedures are not suitable for students in academic institutional payment system.

Considering payment systems for academic institutions, the major responsibilities of the payment gateway are accepting the payment requests and authorizing the mobile users for payment services, where the educational institution can provide their own gateway for their payments. The bank associated with the institutions may link with institution’s payment gateway and can support regular payment procedures. Such a transaction will create high level of trust and confidence between the payment user and the PSP. Due to the unique roles of different stakeholders and distinct payment cultures, there is a need for separate payment system for higher educational institutions but security is the major concern.

Hence there is urgent need to design an architecture for mobile payment system with due care on End-to-End security in payment transactions between the client and the banks.

This investigation intends to propose an architecture for Secure Mobile Payment System using Public Key Infrastructure. The architecture designed is well suited to the academic institutions to carry out the payments and financial services, in particular payment of fees by students from the customer’s bank to the institution.
authorized bank where they study using mobile device anytime and anywhere. It is in this context, this research has been carried out with the following objectives.

- To study the existing mobile payment services and systems.
- To design the architecture for end-to-end secure mobile payment system.
- To develop secure payment interface for mobile client application and server application.
- To develop a digital certificate based mobile transaction security using Public Key cryptosystem for the payment system.
- To establish a test bed for testing the fund transfer in real-time for payment of fees through mobile devices.

The Architecture for Secure Mobile Payment System is designed and developed with strong authentication, authorization, confidentiality, message integrity, and non-repudiation by employing Public Key Infrastructure. The device authentication is achieved using X.509 standard public key certificates. The user authentication is ensured using multi-factor authentication approach. The payment is authorized by the payment gateway namely Mobile Payment Consortia System (MPCS) server by comparing the option-id and fee amount. The integrity of the payment data is provided by using hash algorithm such as Secure Hash Algorithm-1 (SHA-1). Finally, the critical security component of the non-repudiation is supported using digital signature of the involving parties. The security architecture is designed for device authentication, client authentication and client/server authentication and which is implemented using Java 2 Micro Edition (J2ME). The proposed architecture facilitates secure communication between mobile client and the servers using Hypertext Transfer Protocol over SSL (HTTPS) connection. The security
protocol of the proposed architecture uses General Packet Radio Service (GPRS) network. The performance of the architecture is analyzed and the results are presented.

1.6 The Organization of Chapters

Chapter II of this thesis provides a detailed survey on security issues on existing mobile payments systems. The security services such as transaction security, entity authentication, transaction privacy and transaction Integrity, and anonymity are discussed. The security mechanisms such as public key infrastructure, symmetric and asymmetric cryptography and biometry are briefly presented.

The proposed architecture for the secure mobile payment system is briefly presented in Chapter III. The architecture provides necessary technical information on acquiring user information, connectivity, authentication, and communication to facilitate m-payments and payment gateway. The architecture includes components and their connectivity. The PKI-based security algorithms and their functionalities are also narrated in this chapter. The security for device authentication, client authentication and client/server authentication is also illustrated in this chapter.

The security algorithms developed for entity authentication, client authentication, client and server authentication and to establish secure communication during the transaction through mobile devices are presented in Chapter IV.

The simulation study of proposed architecture for mobile payment system that has been carried out and also tested with test bed are explained briefly in Chapter V. The test bed is implemented based on multi-tiered architecture. The hardware and
software setup are also presented. Sony Ericsson K750i-java enabled mobile phone is used for testing the secure user-interface through GPRS network. The client-side functionalities are implemented using Sun Java Wireless Toolkit 2.5.2 that supports Mobile Information Device Profile (MIDP) version 2.0 specifications from Sun Developer Network (SDN) for secure transactions by enabling HTTPS connections. The server components are deployed as Java servlets. Bouncy Castle API (BC-API) is adopted for various cryptographic operations. The proposed architecture is tested with Rivest, Shamir and Adleman algorithm (RSA) cryptographic algorithm to measure the time consumption. The computational cost for the proposed model is also analyzed. Finally, the performance of the system is measured in terms of mean response time and system throughput.

The summary of research and conclusion are presented in Chapter VI. A note for future research of this investigation is outlined in Chapter VII. The list of papers published by the author and the list of references are annexed along with the thesis at the end.