REVIEW OF LITERATURE
Chapter II

REVIEW OF LITERATURE

Mobile Payments nowadays play an important role in every transaction at the personal level and professional level. An increasing number of people are utilizing their mobile phones for payments, money transfer, trade and commerce on a daily basis. This has led to a rapid growth in the development of various mobile payment models and systems. Major research efforts were undertaken in recent years to build a secure mobile payment solution. Current research on mobile payment systems mainly focus on the technological aspects of the system, particularly those that are related to the functionality and implementation issues. In recent times, the focus of the research has shifted to the business aspects of mobile payments such as user adoption process, strengths and weaknesses of the existing system encompassing various dimensions namely transaction costs, size of payments, payment time and security.

Security in payment system is an important requirement in the field of e-commerce secure information exchange and safe financial transactions through mobile networks. However, it is difficult to strongly authenticate the mobile users remotely and provide an adequate level of non-repudiation of transactions. The industrial consortia such as Mobey Forum considered security as a fundamental requirement for mobile payments and financial services when adopted by all stakeholders [Mobey Forum 2010]. Hence, this chapter, before designing high end security architecture for mobile payment system for higher academic institutions evaluates...
and reviews the existing mobile payment system architectures, system models, and security protocols.

Several studies have been conducted till recently to implement more effectively secure mobile payment system in diversified applications. Different mobile payment systems as for examples mobile phone-based system, Subscriber Identity Module (SIM) or Smart card-based system, Point-of-Sale (POS)-based system, and Mobile wallet are found in the market [Britto et al. 2009]. The Mobile Phone-based system can be classified further into Bank Account-based System, Credit Card-based System and Mobile Network Operator (MNO)-based System. The payment systems are classified as shown in the Figure 2.1.

Figure 2.1: Types of Existing Mobile Payment Systems
2.1 Mobile Payment System Architecture

Security is the vital issue for mobile payment system right from the architecture. Guo (2008) has proposed a layered architecture for SMS-based mobile payment system, wherein the payment is done through fund transfer between the consumer bank account to the merchant account. This architecture includes four layers namely load-bearing layer, network interface and core application platform layer, business layer and decision-making layer. Figure 2.2 shows a detailed view of the components and their interactions.

![Figure 2.2: Four layered Architecture for Mobile Payment Systems](image)

The load-bearing layer considers various technologies and infrastructures for data transmission such as Global System for Mobile Communications (GSM), General
Packet Radio Service (GPRS), 3rd Generation (3G) and so on. The secure communication between consumer, content provider and financial institution are handled by network interface and core application platform layer. The business layer includes all application business logics. The decision-making layer uses various tools like statistical analysis and data mining for analyzing the payment market and to help decision on market.

The architecture presented in this system uses Short Message Service (SMS). The transaction details are usually sent as an SMS message. The main issue identified in this architecture is missing of encryption for the data during On-The-Air (OTA) transmission between the service center and the mobile phone. Also, SMS messages can be easily forged by operator network insiders, and thus cannot ensure either confidentiality or data integrity.

The architecture, namely SIMPA, is based on Session Initiation Protocol (SIP) for next generation mobile phone networks developed by Zhang et al. (2008). SIP is designed as the signaling protocol for the 3G mobile networks with the support of Multimedia services including Voice over IP (VoIP) and Instant Message (IM). SIMPA architecture supports Person-to-Person (P2P) payments and traditional security properties such as privacy, confidentiality and integrity. SIP provides a more security support for mobile payment services using Hyper Text Transfer Protocol (HTTP) Digest, Secure/Multipurpose Internet Mail Extensions (S/MIME) and IP Secure (IPSec). The Payment Gateway (PG) authenticates the customer with Personal Identification Number (PIN). The SIMPA architecture is depicted in the Figure 2.3.
However, the limitations in SIP network are lack of floor control within a session and minimal capacity of exchange [IXIA, 2004]. Transport Layer Security (TLS), IPSec and S/MIME which are the underlying security mechanisms in SIP protect only outside attack and not inside attack.

Li et al. (2008) have proposed an architecture for POS payments that supports strong platform attestation with the help of Trusted Computing (TC) technologies. The platform attestation refers to the validation of actual payment application and its respective runtime environment with Trusted Computing. This prevents the mobile devices from the malicious payment software. The architecture employs two techniques namely Identity-Based Signature scheme (IBS) to verify the mobile platform’s integrity and attestation cache to reduce the attestation overhead in order to improve the performance of the payment transaction without sacrificing the security requirements. The following Figure 2.4 represents the Trusted Computing architecture.
Although TC has emerged several years before, it has not yet been widely deployed owing to adverse views [Cheng et al. 2008]. In addition to that the merchant uses Near Field Communication (NFC) at Point-of-Sale (POS) terminals to transmit the payment information. However, the NFC works at very short distances and only supports peer-to-peer communications. This payment system has been in use but transactions are too slow for commercial implementations and phone-to-phone transactions take approximately 6 seconds [Gauthier et al. 2009].

Xi et al. (2007) have proposed an architecture for SIM-based mobile payment system using SMS technology, where the payment application is installed into the SIM card of the mobile phone. The interoperability between SIM card and terminals is achieved through GloalPlatform standards [Ashutosh et al. 2005].
There are many drawbacks on this system. The smart card remains unblocked until
the phone is switched off or the SIM loses power. Second, when the mobile phone
or SIM is lost or stolen, the user has to inform the operator immediately. The above
payment system architecture supports symmetric cryptography. However, this does
not satisfy the transaction security properties. The confidential information such as
account number and password are sent through the message which falls into
eavesdropping in a radio environment.

Liu et al. (2006) have proposed the architecture for Mobile Payment System based
on Radio Frequency Identification (RFID) technology. This type of mobile
payment services have adopted this technology launched by NTT DoCoMo in Japan
and MONETA service launched by Sun Kyung (SK) Telecom in Korea. The
proposed architecture uses RFID tags to communicate the user with POS terminal,
where the RFID tags are available at mobile device and the RFID reader is
integrated with POS terminal. The RFID POS terminal establishes the
communication with Mobile Payment Platform (MPP) over GPRS network. RFID
tag uses smart card technology with Chip Operating System (COS) to support
public key infrastructure, mutual authentication and data encryption. The proposed
system provides major services such as E-ticket, ID service, Mobile Insurance,
Mobile bank transactions and so on. The architecture for GPRS mobile payment
system using RFID is presented in the Figure 2.5.
Figure 2.5: Architecture of GPRS Mobile Payment System using RFID

However, the major limitation in RFID technology is the memory size of the card. Since the proposed architecture supports GPRS, many security risks are posed at network level such as GSM threads like Hijacking the outgoing calls, Eavesdropping on user data and compromised cyber key, system intrusion, Internet junk data, denial of service. The connectivity problem is also another important issue for the users.

Gao et al. (2005) have proposed the architecture for peer-to-peer m-payment system using symmetric key mechanism. The system allows the customers to make payments over the wireless Internet or via Bluetooth communication. The proposed solution employs security mechanisms such as service registration, access control,
security code attachment, and speaker verification. The user registration can be done through either online or mobile. The mobile user is authenticated by verifying the P2PID and password, where the verification of user, voiceprint are for future device authentication. The sensitive data such as user ID, password, PIN, account number, etc., are encrypted using shared secret key between the communicators. The authentication key is digesting using Message Authentication Code (MAC). The system deploys voice verification as a security component using hypothesis-testing problem where the system has to accept or reject based on claimed identity utterance. Figure 2.6 presents the system architecture for P2P paid payments.

![System Architecture for P2P-paid payments](image)

Figure 2.6. System Architecture for P2P-paid payments

However, this verification mechanism will fail when the legitimate user’s voice is changed. The major drawback of this architecture is that the symmetric key mechanism adopted for encrypting and decrypting the payment transaction does not
support transaction security properties. This method is easily vulnerable to the attack by the illegitimate users and has potential security risks.

Labrou et al. (2004) have proposed the architecture for server-side wallet which is built on Universal Pervasive Transaction Framework (UPTF). UPTF is a generic architecture and defines communication protocol, called the Secure Agreement Submission (SAS) that supports multi-party agreements over the insecure wireless networks. The UPTF SAS protocol encrypts the message using symmetric, shared-secret-key approach and the secret key is known only to an individual party and the trusted third party, namely the Secure Transaction Server (STS). STS maintains a log of all messaging activity for non-repudiation purposes.

Since the proposed architecture is based on server-side wallet, the scheme does not store any personal information at the mobile devices; however the user needs to enter the PIN for the payment authorization. The Figure 2.7 represents the server-side wallet architecture using Universal Pervasive Transaction Framework.

![Figure 2.7: Wallet architecture using UPTF](image)

As in Figure 2.7, Ch A is typically a wireless channel to accommodate the communication between the payer and payee and which is not secure. The channels
B and C are the links between the Payer and the STS and the Payee and the STS, respectively where the communication is done through the Internet. The channel D is assumed to be a highly secure communication path, such as a Virtual Private Network (VPN). To support physical POS payments, the Universal Pervasive Transactions Device (UPTD) was designed to wirelessly connect with the POS terminal using an 802.11b Wireless Local Area Network (WLAN) radio and allowed to make purchases and payments with them. The wireless wallet application is implemented using Java 2 Micro Edition (J2ME) and Hyper Text Transfer Protocol (HTTP) that is adopted for secure communication. The security mechanism is supported by J2ME and the scheme uses HTTP for communication between the payer and STS server. This provides an avenue for Man-In-The Middle (MITM) attack by the impostures.

Karnouskos et al. (2003) have presented an architecture and a business model for Secure Mobile Payment System (SEMOPS), where banks, mobile operators, customers, merchants, developers, initiators, license holders, service providers and suppliers are the key actors. The SEMOPS is the universal and open mobile payment system that supports micro, mini and macro payments. SEMOPS supports the business opportunities inherent in billing, customer-service, technical relationships and banking services among mobile customers, mobile operators and banks in order to offer a competitive solution to existing payment services. SEMOPS supports both mobile and Internet transactions, and can accommodate various transaction types, irrespective of value, function, time, and currency. The SEMOPS architecture is depicted in Figure 2.8.
A notable limitation in SEMOPS model is that the customer has to prepare a Payment Request (PR) and submit it to the customer payment processor. The customer payment processor then prepares a payment notification and forwards it to the Data Center (DC). Since the payment notification relays through DC and merchant payment processor, the transaction data casts a trail on the way to the merchant. Then the customer and the merchant have to trust the payment processors, but there is no guarantee for payment processors. Hence, this model is not commonly used.

Antovski et al. (2003) have presented the architecture for Mobile Network Operators (MNOs) based payment system. The architecture utilized asymmetric key encryption and Public Key Infrastructure to protect the payment data and HTTP method was used for data transmission. The system uses J2ME and the authors have
assured that J2ME technology is suitable for building successful mobile payment systems. In this payment model, the payment transaction is initialized by the merchant by sending a message to the bank.

The proposed architecture in this system does not include the payment confirmation process by the customer. The HTTP protocol is used for communication between the entities that leads to high security risks such as server-side HTTP attacks and client-side HTTP attacks. In 'HTTP Connect Tunnel' attacks, the HTTP-connect-tunnels are used for sending spam emails [SANS 2009]. In the MNO-based payment system, when the payment amount is transferred from one account to another in different mobile operator’s network, it involves additional procedures for validation and clearing. This leads to high cost and hence not suitable for micro-payments. The system suffers seriously due to lack of compatibility with different MNOs, high demand for privacy, authentication and trust-management protection, and lack of scalability.

2.2 Mobile Payment Models

There are a number of mobile payment models found in the market and they are categorized into theoretical model, scenario-specific model and open or scenario-independent model [Jun et al. 2005]. The theoretical model generally provides a layered or module-based framework that illustrates the payment procedures, principles and security issues only [Zheng et al. 2003]. Scenario-specific models are classified into disconnected interaction model [Isaac et al. 2007], client-centric model [Astudillo et al. 2009], server-centric model and Kiosk centric model [Isaac et al. 2006]. In these models only protocol design entities have interaction with each
other in a restricted way due to security challenges. These models focus on application’s scenario specific that limits the extensibility. The models like Mobile 3-D secure, PayBox, Mobile ticket, Top-Ups fall into to this category. The Open or Scenario independent models integrate the legacy infrastructures and tackle the security and privacy issues.

Meng et al. (2008) have proposed a secure payment model for credit card-based mobile payment system based on Wireless Application Protocol (WAP). In this model, Elliptic Curve Cryptography (ECC) algorithm is adopted in order to reduce the time taken for key generation at mobile device and WAP PKI (WPKI) are implemented to secure wireless communications. WPKI is the optimized version of the traditional PKI for wireless networks. The Wireless Transport Layer Security (WTLS) certificate defined by the Open Mobile Alliance (OMA) is utilized for key distribution in the wireless environment. The WTLS certificates do not have extensions and can be stored in Wireless Identification Module (WIM). With cross-certification, the mobile payment system is organized as a Bridge Certificate Authority (CA) authentication model, which is presented in Figure 2.9.

The major issue raised against the Bride CA Authentication model is that each entity requires to download not only their root CA’s certificate but also the trusted neighbours’ CA certificates to verify the identity of the entity. WTLS provides transport level security between a user device and WAP gateway, however there is a need for security protocol translation between the wireless network to the Internet. It paves way for high level security risks for the users. Hence, there is no end-to-end security at the WAP gateway and also the WAP gateway needs to be trusted. The
wider acceptance of the proposed model by the users is limited due to this security lapse.

Jun et al. (2005) have presented a model for mobile payments to conquer the limitations of Secure Mobile Payment Service, which reduces the trust dependence on payment processors and enhances the security and privacy. To avoid disputes with the customers, the customer payment processor preserves the timestamp and Payment Request (PR). The customer and merchant information resides with respective payment processors. This supports privacy and anonymity for both customer and merchant. The transaction data are hashed before transmission to ensure the integrity. The model presented here is introduced Certificate Authority along with Time Stamping (TS) service to ensure the non-repudiation and transaction accountability. The Figure 2.10 represents the architecture proposed by the authors.
Study reveals that the proposed model uses third party to reduce trust dependency that requires extra processing steps as well as additional transaction cost. The major threats like cracking/hacking, viruses, worms, Trojans, and Spyware are possible to send by the falsified third-party organisations or individuals. Those attackers are classified as insiders, intruders, once-removed parties and their intention is to harm the payment transactions and networks. The method for certificate validation is another major concern for high-level security.

Salvi et al. (2002) have suggested three different payment models for Wireless Service Provider (WSP) such as Intra-WSP, Inter-WSP (National) and Inter-WSP (Global). The payment service can be either prepaid or post-paid. In the Intra-WSP, both the payer and payee carry the payment transactions with the same wireless service provider. In the Inter-WSP (National) model, the group of WSPs facilitates
payment services to their subscribers and this model is divided further into two types. The type-1 in Inter-WSP (National) model provides payment services, where the customer and merchant are subscribers to the different WSPs in the same circle. The type-2 of Inter-WSP (National) model includes different WSPs in different circle for their subscribers. Finally, in the WSP-global model, the subscribers avail International roaming payment service that supports the global issues like currency exchange rates and legal bindings. Those models depend more on mobile network operators for authentication. End-user identification is based on the PIN once mobile device power-on. Considering that most of the time the phones are ‘on’, there is no reliable end user authentication if phones are lost or stolen.

2.3 Security Protocols

The specification of mobile payment protocols guarantee the secure communication between the parties involved in payment transactions. Godbole et al. (2008) have proposed the security protocol to support the micro-payments for Secure Mobile Payment Service. The suggested micro-payment protocol uses intermediaries to aggregate micro-payments and thus achieves efficiency and reduces low cost per transaction. The customer needs to authenticate himself to the Customer Payment Processor (CPP) using PIN. To achieve non-repudiation, CPP digitally signs each Payment Notification (PN) and sends it to the Merchant Payment Processor (MPP) through Data Center (DC).

This protocol uses weak method to achieve atomicity due to the messages that get lost when the timer will expire. The proposed protocol fails to support the security mechanism if the customers do not pay their amount. The usability of the payment
service is also seriously affected by the protocol when the users maintain the enough balance in their account against the purchases.

The enhancement of payer's privacy protection is one of the most significant security services for the mobile payment systems. If the payment system does not support privacy, the customer identity and transaction details are revealed not only to the merchant but also to payment gateway and the banks. Fun et al. (2008) have proposed a private client-centric payment protocol for restricted scenarios using the symmetric key operations. The protocol protects the payer's privacy from the eavesdroppers that includes identity privacy protection and transaction privacy protection. In order to protect the payer's identity, a random number is sent along with the transaction identity to the payee and one-time ID generation and shared session key are used applied to achieve transaction privacy.

The proposed protocol consists of two sub protocols such as registration and payment protocol. The registration protocol uses two factor authentication mechanism such as PIN and password. The payment protocol is based on Credit Push Model, where the payment application will allow consumers to make purchases from online merchants as well as pay bills using direct debit via automated clearing house.

Study reveals that the protocol runs on symmetric-key operations requiring low computation at all engaging parties, but the protocol is not good enough to support transaction security properties provided by public-key based payment protocols such as Secure Electronic Transaction (SET) and iKP.
Peláez et al. (2008) have proposed efficient protocol for micro-payments which is based on anonymous mobile cash. The protocol uses RSA based blind signature scheme and the hierarchical authentication model. The protocol consists of five phases namely enrolment phase, withdrawal phase, purchase phase, payment phase and deposit phase. In the enrolment phase, pseudonym certificate is used to identify the customers where the certificate includes Customer’s Name (CN) and the identity of SIM card. In the withdrawal phase, the communication between the customer and bank is carried out through an Automatic Teller Machine (ATM) using Bluetooth technology and the customer can define various denominations. The security scheme presented in this protocol prevents the double spending and forgery attacks. Using the shared symmetric key between the customer and ATM, the secrecy and authenticity are achieved. In the purchase phase, the same Bluetooth technology is used for communication between the customer and the POS.

Since the proposed protocol uses pseudonym certificate for authenticating the users, the bank signs and manages pseudonym certificates for each member of the group. The bank stores the certificates in a public repository. It provides extra responsibilities for the banks and involves additional cost for them. The wider acceptance of this security protocol is limited due to no standard of pseudonym certificates.

The Secure Electronic Transaction supports single-factor authentication mechanism for online payment systems, however the single-factor authentication is inadequate for security to transfer the funds in wireless environment. To solve this issue, Tiwari et al. (2007) have proposed the security protocol for wireless payments that
supports multi-factor authentication scheme and also achieves usability. The multi-factor authentication mechanism provides strong authentication, where the security protocol uses Transaction Identification Code (TIC) and SMS Confirmation with one-way authentication and two-way authentication. The SET protocol suffers serious security vulnerabilities when the mobile agents are roaming in the network.

Aboud et al. (2007) have proposed the protocol for anonymity, non-repudiation and traceability to avoid extortion attacks. A blind signature scheme is used to achieve anonymity, where the blind signature is a form of digital signature in which the content is blinded before it is signed. The blind signature scheme is generally based on the relations among the bank, user and blind office, because both blind office and bank are impersonating the users without being noticed. The major problem with this current protocol is difficulty in keeping the trust relations between blind office and bank when the user claims for repudiates. This leads to critical situation among the involving entities. Although the proposed protocol avoids impersonating the user by blind office and bank, the user computational cost is heavier than the existing protocols.

Other security protocols available for wireless communication are Authentication and Key Agreement protocol (AKA) [Lee et al. 2000], ASPeCT protocol [Newe et al. 2003], Boyd-Park protocol [Tin et al. 2003], SET protocol, iKP protocol, NetBill [Ogata et al. 2004] and Beller, Chang, Yacobi (BCY) protocol [Kim et al. 2005]. The VISA and MasterCard have proposed two payment protocols namely Visa 3D Secure and MasterCard Secure Code for card-based mobile payment system. Pasupathinathan et al. (2006) have evaluated these Visa 3D Secure and
MasterCard Secure Code protocols using formal method tools namely Casper and Failures-Divergences Refinement (FDR). MasterCard protocol supports more security for session management, tokens generation, and automatic form-filling. Visa 3D secure protocol supports basic and proven solution using PKI’s and certificates. However, it is inefficient for processing the on-line payment transactions due to network delays and time-outs.

Kim et al. (2005) have analyzed BCY, the Carlsen BCY and the Mu-Varadharajan BCY protocols using the formal method tools such as Communication Sequential Processes (CSP), Casper and FDR. Original BCY and Carlsen BCY protocol suffer due to the security vulnerabilities like key agreement, replay attack and entity authentication. Mu-Varadharajan BCY protocol suffers from key freshness problem because it uses the same session key during the communication. Further, the authors have proposed a revised Mu-Varadharajan BCY protocol that supports mutual authentication and key agreement between the involving parties. The protocol uses Diffie-Hellman algorithm for key exchange with the Modular Square Root (MSR) for encryption, which reduces the computational burden on mobile device. The user authentication is achieved by Challenge-Response mechanism. However, the BCY protocol suffered from man-in-the-middle and replay attack.

The agent-based protocols such as SET/A, SET/A+ and LITESET/A+ [Pang et al. 2002] support multiple payments by conducting individually to each merchant for multiple times. Wang et al. (2005) have proposed a secure payment protocol, namely LITESET/A++ that supports multiple payments and applies Signature-Share scheme and Signcryption-Share scheme. Signature-Share scheme is adopted to send
the Order Information (OI) securely, where the cardholder’s signature private key is divided into two parts. The first part is kept by the cardholder. The second part is send to the Trusted Third Party (TTP) for generating shared signatures. Signcryption-Share scheme is used to sign the Payment Information (PI) and then PI is sent to the Payment Gateway (PG) as an encrypted way using temporary session public key. The over-spending and over payment attacks could be prevented by verifying the amount mentioned by the TTP and the Merchant at PG. However, the major drawback in this security protocol is that the part of the cardholder’s private key is also revealed to TTP. This violates the policy of private key mechanism and there are chances to eavesdrop the information by illegitimate users during the transmission.

Kungpisdan et al. (2004) have evolved an account-based payment protocol using symmetric key cryptography. The limitations considered by this protocol on mobile devices are lower power, storage and computational capabilities and the limitation of wireless networks like low bandwidth and reliability, and higher latencies. Since the protocol employs a symmetric key mechanism, it can be deployed with lower computational devices at all engaging parties and can avoid additional communication process, whereas in PKI, the certificate is verified with Certificate Authority. The proposed protocol contains two sub-protocols namely merchant registration protocol and payment protocol. The proposed protocol made an attempt to support the transaction security using symmetric encryption with secret key. Transaction integrity is achieved using Message Authentication Code (MAC), and Non-repudiation of transaction is supported by shared secret key. The proposed protocol used only the shared secret key for non-repudiation. Since the secret key is
shared between the customer and merchant, there is no authenticity for the payment transactions.

Wang et al. (2003) have offered a Secure Wireless Payment Protocol (SWPP) to overcome the security vulnerabilities in Wireless Payment Protocol (WPP). SWPP supports security mechanisms using Wireless Transport Layer Protocol (WTLS) and digital signatures. The customer uses Wireless Identity Module card to store all confidential data which are bank information and private keys. In SWPP, secure WTLS session channel is built between the customer and the bank gateway. The customer authorization in SWPP is implemented using the WMLScript signText function.

A major problem with the protocol is that the invoice is not signed by the merchant. Although WTLS ensures the integrity of the data when communicated, it could not prevent any party forgery messages, if they are not signed. In addition, the order information Order Information (OI) is not signed and this provides a chance for the merchants to forge the customer request. Consequently, the protocol design considers the bank as a trusted party, but if any messages come from the bank without sign, the customer does not trust them and false financial institution can perform a man-in-the-middle attack.

2.4 Mobile Payment Systems

Researches undertaken on existing payment systems have made an attempt to improve security services as each system has limitations.
Wang et al. (2008) have demonstrated J2ME based Mobile payment system using PKI that achieves security in payment process through multi-party digital signature. The proposed system is based on server-side wallet and the payment server performs key generation, validation, storage and communication. Three major functions supported by it are pay module, buy module, and accounting module and uses multi-digital signature. The user is authenticated by verifying the signature. The activities involved in the multi-signature process are signature initialization, generation and verification. The protocol considers the security issues like eavesdropping, falsifying, tampering and resending. The eavesdropping is prevented during the transmission using PKI. The digital signature is applied to prevent from forgery. The digital signature and time stamp are used to achieve the message integrity, where the timestamp prevents replay attack.

In this system, the mobile user sends the PIN to the service provider for confirmation of payment request. This provides the chances to the attackers to steal the message like PIN. Additionally, in the proposed system, the service provider expects response from the mobile user within two minutes for payment confirmation. If the network connectivity fails during the payment transaction, the user is unable to responds within two minutes. On account of this, the legitimate user will suffer and he has to bear the network connectivity charges repeatedly till the payment process is completed.

Hassinen et al. (2008) have proposed a mobile payment system that uses national public-key infrastructure, namely the Finnish Electronic Identity (FINEID). Further, the authors have proposed two protocols for virtual POS payments and for
real POS payments at vending machines for buying train tickets. The proposed system brings about constraints for the customers to make use of the services like the customers must get the SIM card only from the mobile network operator and they must register it at a police station. To support virtual POS payments, the merchant has to implement a web service for processing mobile payments and to avail the real POS payments, a number of changes have to be implemented at vending machines. To enable the protocol between the customer and the bank, the bank must implement the protocol and accept authentication with the FINEID card, and to support mobile payments with PKI-SIM cards, additional software must be implemented and deployed at the bank servers. This severely affects the usability of the customers.

Another major limitation of the system is that the user authentication is done with the participation of mobile operator using PIN. Thus, the mobile operators charge both customers and service providers for authentication. Additionally, the Bluetooth technology is adopted for real POS payments at vending machine. Bluetooth operates in the unlicensed 2.4 GHz band and the security mechanisms provided by Bluetooth need to be ascertained.

Garner et al. (2006) have formulated XML-Enabled Payment System (XEPS) namely, ClearCommerce that supports remote macro-payments using GPRS. The proposed system is based on client-side wallet. The ClearCommerce provides an XML-based payment API for the users to send their complete transaction information to the financial institutions. Once the user provides the necessary information, the web server generates XML document for the payment transaction
along with order information, delivery address, total price, etc. and the product
delivery address is mapped with credit card address for user authentication by the
bank. Once the basic validation is completed, the status of the transaction is
returned to the merchant as an XML document by the financial institution. The
major disadvantage of the proposed system is its weaker user authentication method
by verifying address of the credit card. If any changes are made in the address on
the credit card, the legitimate user can not avail the payment services.

Yun et al. (2005) have proposed the client-side wallet using MobileC that operates
on General Virtual Machine (GVM). GVM is a virtual machine platform that
executes the applications dynamically on mobile device. GVM payment system
includes GVM Software Development Kit (SDK), GVM server and mobile device
with GVM module as built-in. GVM SDK is a tool to produce GVM applications
that includes MobileC compiler, Media Tool Kit and GVM emulator. The payment
process is composed of initialization process and transaction process. The
initialization process includes download of payment system, certificate and credit
card information to mobile device. The transaction process handles communication
between server and mobile device. Finally, the authors have discussed
implementation details along with the results. However, the GVM platform is not
deployed widely. This limits the wider acceptance of the proposed wallet.

Having reviewed the literature, it is evident that several architectures, models,
protocols and systems exist but each one faces several limitations in the payment
procedures. There is no wider acceptance of the payment system due to the lack of
adequate security during the transaction at both ends. The study also reveals that the
An Architecture for Secure Mobile Payment System using Public Key Infrastructure