Chapter 1

Introduction

1.1 Background

1.1.1 Mobile Commerce

Internet technology offers extensive ranges of services such as electronic mails, file transfers, etc., and one of the most popular services offered on the Internet is Electronic Commerce” (or e-commerce). E-commerce is becoming bigger technological wave that has changed the way by which business is being conducted. Two main areas in which e-commerce grew significantly in recent years are Internet banking and conducting business on the Internet [1]. With Internet banking, the way customers make use of banking services has changed. They do not have to go to ATM (Automatic Teller Machine) terminals or stay in-line at a bank branch to withdraw or transfer money between accounts, but simply log on to a bank’s website which provides Internet banking services including withdrawing money from the customers’ accounts. Although the customers cannot get physical cash in their hands, they are able to transfer money to electronic cards and bring them to purchase goods or services at stores. Moreover, the customers are able to pay bills or schedule monthly bill payments by using the Internet banking services. Regarding conducting business on the Internet, basically, e-commerce simulates and enhances traditional ways that people conduct business or communicate to one another into electronic manners. For example, electronic mails
(e-mails) replace mailing services in that people do not have to wait overnight for delivery of letters, but only in minutes electronically. Most of the features of e-mails are similar to paper mails such as (digital) signatures of senders, timestamps, or returned mails in case the mails cannot be received by the recipients. In addition to the time reduction, e-mails reduce the cost for document and delivery.

According to business transactions, many e-commerce websites enable their customers to browse for goods and services offered in their virtual stores remotely from the customers’ personal computers. Not only physical goods, such as books (e.g. www.amazon.com) or laptop computers (e.g. www.dell.com), are offered, but electronic goods, such as music, digital images, video clips, or electronic novels, are also available. Customers simply select desired products or services and pay for them by credit-cards or electronic cash cards. More importantly, these virtual stores are open 24 hours a day, 7 days a week. Recently, e-commerce transactions can be performed on the move. The emergence of wireless communication technology offers the ability to access the Internet in order to perform e-commerce transactions through mobile devices e.g. cellular phones, PDAs (Personal Digital Assistants), or laptop computers. Such mobile devices are connected to the Internet via modems or wireless network adapters. This greatly offers convenience to users to perform e-commerce transactions from distance at any time. Performing e-commerce transactions where at least one engaging participant in an e-commerce system is a mobile user is called “Mobile Commerce” (or m-commerce). Recently, m-commerce has been receiving attention considerably and has high growth rate. A recent study from IDC, a market intelligence and advisory firm, forecasts that the US m-commerce market will reach US$58.4 billion by 2007 compared to US$127 million in 2001 [2]. Compared to conducting e-commerce over fixed-networks, m-commerce offers many advantages [3] which include:

- Users in a m-commerce system can access the Internet to perform e-commerce transactions through their mobile devices in real time at any place.

- Mobile devices have smaller size and lower weight than personal computers (PCs). Thus, they can be easily brought with users to anywhere.
• Mobile devices are personally used so that they can be personalized to fit the needs of particular users.

1.1.2 Mobile Payment

Although e-commerce is not all about fund transfer, electronic payment (or e-payment), such as credit-card payment over the Internet, is still one of the most popular e-commerce applications. In other words, e-payment is one of the crucial parts of an e-commerce transaction in that the e-commerce transaction cannot complete without it. For example, an online book store which provides both electronic and physical books to its customers must have a supporting payment system available for its customers to transfer money to it. Therefore, each customer can complete the purchase which includes goods delivery (or commitment of goods delivery) and payment with the store in one transaction. Without the payment system provided, the customers are required to perform two sessions separately: one for the goods purchase and the other for the payment transaction. In particular, the payment transaction has to be performed by transferring money to the store’s bank account directly. E-payment is an alternative to traditional payment which has been generally performed physically by presenting a credit card to a merchant and signing on a payment slip as evidence of the payment transaction made to the merchant.

As briefly described in the previous section that there are several kinds of e-payment methods, the most primitive payment method is fund transfer between bank accounts. According to this method, an e-commerce website sends an invoice to a customer via an e-mail and requests the customer to transfer the money as the payment for the requested goods or services to its bank account. After receiving the payment, the website sends the corresponding payment receipt via the customer’s e-mail and delivers the goods to the customer. It can be seen that the customer commits the purchase to the website online, but the payment is performed off-line. Later on, e-payment has been developed to fully online transactions such as credit cards, electronic checks, electronic cash, and micropayment. The most popular type of e-payment methods is credit-card payment. According to this method, after selecting preferred goods from an online store, a customer can make a payment via a supporting credit-card payment system provided by the store by simply filling in her
credit-card number and relevant information, such as date of birth or billing address, for authentication and payment authorization purposes. Such information is transferred to the customer’s credit-card company to check for credit availability. If the request has been approved, the goods (in case of electronic goods) and corresponding receipt of payment are transferred to the customer shortly. Mostly, this kind of payment systems is operated using 128-bit SSL (Secure Socket Layer) protocol [4].

Credit-card payment systems such as SET (Secure Electronic Transaction) [5] provide more secure payment transactions than SSL-based payment schemes [4]. In SET, in addition to holding a valid credit card, a customer needs to install SET payment software (called SET wallet) on her computer. After browsing for goods or services from a SET supporting online store, the SET wallet installed on the customer’s computer is activated. After filling necessary payment information, the SET wallet performs highly secure cryptographic operations e.g. public-key cryptographic operations, to generate a purchase request. This request is transferred to the store and the customer’s credit card company for payment authorization. After getting an approval, the requested amount is transferred from the customer’s account to the store’s account and the customer then receives the requested goods and the corresponding payment receipt at the end of the transaction. Credit-card payment seems to be a simple method to make a payment for goods or services on the Internet because many people have credit cards and regularly use them to purchase goods or services in physical stores. However, the credit-card payment systems have high operational cost, especially at the merchant side. As a result, credit-card payment is not suitable for low-valued payment transactions.

Alternatively, a payment method that is suitable for low-valued transactions is called “Micropayment”. Most micropayment systems deploy low computational cryptographic operations and simple message passing in order to reduce operational costs. The examples of micropayment systems are Millicent [6], PayWord [7] and PayFair [8]. Electronic payment in wireless environments introduces the term Mobile Payment” which is defined as interactions among engaging parties in a payment system regarding a payment transaction where at least one engaging party is a mobile user. With mobile payment, obviously, customers can purchase electronic books from an online
publisher, that has the system supporting the payment from mobile devices, while they are on the move. Due to the fact that mobile payment represents e-payment, previously performed in fixed environments, in wireless environments, it offers the same services as that offered by e-payment. However, due to the constraints of wireless environments, low-valued payment methods, such as micropayment, which have lightweight operations and low operational cost are likely to be more suitable for wireless environments than other methods.

Electronic payment, including mobile payment, plays an important role in e-commerce in that it is relevant to fund transfer among engaging parties after having an agreement to purchase or sell products or services. It must be performed in a secure manner. Moreover, the security of electronic payment system is also one of the most concerns for customers to make online payment with online stores.

1.1.3 Process Oriented Architecture

Process-Oriented Architecture (POA) is a term used to describe the philosophical approach to process interaction and management. The POA contains a set of core elements, such as business processes and sub-processes, associated business rules, and components used to sustain business performance, deliver a consistent experience, and enable continuous improvement. An effective POA is considered the foundation of process focused organizations, and enables enterprise visibility, alignment and scalability.

The Process-Oriented approach uses several architectural guiding principles to construct process ecosystems that business users can dynamically combine and compose into processes that meet continuously evolving and changing business requirements. The following guiding principles define the ground rules for development, maintenance, and usage of the POA:

• **Loose Coupling** - The principle of Loose Coupling places emphasis on reducing dependencies between processes, procedures, and their related components. The primary goal is to reduce the risk that a change made within one process will create unanticipated changes
within other processes. Limiting interconnections can help isolate problems when things go wrong and simplify maintenance and troubleshooting procedures.

- **Process Reusability** - The principle of Process Reusability emphasizes creating processes, procedures, and related process elements that have the potential to be reused across the enterprise. This reduces the risk of rework so that organizations can adapt more quickly to industry changes.

- **Process Granularity** - The principle of Process Granularity places emphasis on a design consideration to provide optimal scope and the right level of detail when documenting processes, procedures and any related process elements. It is important to design processes with the right granularity so that end users can easily locate and use necessary materials.

- **Process Discoverability** - The principle of Process Discoverability emphasizes making processes discoverable by adding interpretable meta-data to increase process reuse and decrease the chance of developing processes that overlap in function. By making processes easily discoverable, this design principle indirectly makes processes more interoperable.

- **Process Autonomy** - The principle of Process Autonomy emphasizes the creation of processes which carry out their capabilities consistently and reliably in real world situations. By fostering design characteristics that increase a processes reliability and behavioral predictability, they are less likely to produce issues which force reactive responses once deployed.

- **Process Composability** - The principle of Process Composability emphasizes the design of elements such as sub-processes in a manner so that they can be reused in multiple processes that are themselves made up of composed elements.

Benefits of a Process Oriented Architecture include:

- **Becoming More Agile** - Process-Oriented architectures enable organizations to respond quickly to new business imperatives, develop distinctive new capabilities and leverage existing processes for true responsiveness.
• Reduced Maintenance - Maintaining a sub-processes or process component as a contained element simplifies the task of maintenance. Changes can be made once and in one place for all business processes that use the component, reducing the effort required to make modifications.

• Reuse of Corporate Assets - Process-oriented architectures promote the reuse of existing assets, increasing efficiency and reducing process development and improvement costs.

• Streamlined Costs - Introducing POA within an organization frees up resources and helps to ensure that investments are focused on core capabilities aimed at growing the business instead maintenance and modifications to multiple processes.

• Shorter Development Times - The major benefit of re-use is shorter process development times and also reduced development costs. Development times are also compressed because, while they must conform to a consistent architecture, elements from one process can be used in another.

• Maximizing ROI on Legacy Processes - Providing a level of re-use, wrapping a legacy process with newer elements created for other processes can prolong its life, allowing an organization to maximize its investment in legacy business processes that cannot easily be thrown away.

• Simplified and Productive Process Development - A unified, easy-to-use set of process components enhances process productivity, promotes asset re-use, and fosters enterprise collaboration.

• Unified Process Management and Monitoring - A Process-Oriented Architecture using shared components and cross-process end-to-end tracking help provide integrated governance and security.

• Clear and Comprehensive View of an Organization’s Resources - Relationships between People, processes, systems and goals are easily understood and changes can be quickly and easily analyzed and implemented.
1.2 Security and Limitations of Mobile Payment Systems

Generally, two main reasons explain why securing mobile payment systems is not accomplished: limitations of wireless environments and security of the mobile payment systems themselves as shown in sections 1.2.1 and 1.2.2, respectively.

1.2.1 Limitations of Wireless Environments

Performing payment transactions in wireless environments mainly suffers from resource limitations of mobile devices and characteristics of wireless networks [9],[10],[11].

Mobile devices have the following limitations:

- Computational capability of their processors is comparatively lower than that of personal computer (PCs).
- They are operated using battery power compared to electric power in PCs. Therefore, they can stay operated for shorter period than PCs.
- They have limited storage which affects available cryptographic algorithms applied to them.

A mobile device with the above limitations is not capable of performing high computational cryptographic operations such as public-key operations which are used in a fixed-network device such as a PC. Due to the low computational capability of mobile devices, completing a payment transaction on a mobile device takes longer period of time than that on a PC which has higher processing capability. Moreover, public key operations are required to have certificate verification processes which require storage on each mobile device to store public-key certificates.

Although recently, mobile devices with high computational capability such as smart phones or powerful, wireless-enabled PDAs, have been launched to the market, they are still unattracted by users. The research conducted by IDC [ITF] states that estimated 650 million mobile phones are expected to be sold in 2004. Among these units, 30.05% of them are WAP-enabled phones (around
195 million phones) [12]. Whereas the number of high computational capability mobile devices such as smart phones and PDAs to be sold in 2004 are less than WAP-enabled phones; only 17.6 million smart phones are expected to be sold in 2004 [ITF] and 11.367 million PDAs are to be sold and expected to decrease to 11.251 million units in 2005 [13].

Wireless networks have the following characteristics:

- Wireless networks have lower bandwidth than fixed networks.
- Network connections over wireless networks are less reliable since packet losses occur more frequently than that of fixed networks. Packets need to be retransmitted which may result in high latency.
- Connection cost of wireless networks is higher compared to that of fixed networks.
- Data transmitted over wireless networks is easily eavesdropped.

From the above limitations, mainly due to poor performance, performing payment transactions over wireless networks is time-consuming. Moreover, performing payment transactions on low computational capability mobile devices will spend longer time to complete each transaction. As the connection cost of the communications over wireless networks is much higher than that over fixed networks, performing payment transactions over wireless networks using such mobile devices will charge users a large amount of money on their bills. In addition, due to the fact that the data transmitted over the wireless networks is easily eavesdropped, this can be prevented by applying highly secure cryptographic techniques such as public-key operations. However, Such operations require high computational capability devices and high-speed wireless networks that may incur high cost for users.

1.2.2 Security Vs Transaction Performance of Mobile Payment Systems

Performing electronic payment transactions over wireless networks raises concerns about security of the underlying payment systems. Ideally, both traditional and wireless Internet should serve
all applications, including making payment, with the same level of security. Moreover, mobile payment applications should be compatible with existing infrastructure of traditional electronic payment applications so that the existing infrastructure can continue to operate. However, as discussed in the previous section, performing payment transactions in wireless environments suffers from a number of limitations. A possible solution is to replace high computational cryptographic operations applied to the underlying payment protocol with the lower ones, e.g. replacing public-key cryptographic operations with symmetric-key operations and hash functions, especially the ones operated on a mobile device [14], [15], [16].

This can reduce computational and communication load at the mobile users. However, different kinds of cryptographic operations provide different levels of security. Public-key operations provide non-repudiation property whereas symmetric-key operations do not [10]. Hence, deploying a symmetric-key based payment protocol in the payment system results in the lack of the non-repudiation property. As a result, enabling mobile payment seems to be a trade-off between its transaction performance and security.

1.3 Problem Definition

The market for mobile payment systems is still searching for better ways of handling small value payments, so called micropayments, as used in vending machines. The benefits of having an electronic connection of some kind is apparent, the machines can instantly report the need for repairs or more supplies. Most current systems require a permanent connection to each machine, leaving the system dependant on the connections to the machines. The server handling the service can be protected against denial of service attacks but it would not be cost effective to protect each machine and an attacker could attack each machine separately from the Internet if they all have their own connection. The connection might also fail by unintentional reasons and the machine would then by unusable for mobile payments until this has been repaired.

A security issue that is addressed by this project is the issue of identity theft that otherwise can
be accomplished by monitoring the equipment on the machines in order to copy the authentication information inserted. The most common identification tokens are credit cards that can be used in a wide array of situations to pay for items using the personal identification number associated with the card and that should be known only to the user. The use of credit cards as a payment medium makes mobile payment systems on vending machines very susceptible to attacks as these machines often are unmonitored and can be modified with information theft equipment without the suppliers knowledge, resulting in the theft of payment information for all cards used in the machine during the attack. Therefore, it should be possible and preferable to perform the authentication without making it accessible to an attacker monitoring the machine.

1.4 Research Brief

The thesis is practically based on research work being done towards securing transaction for mobile payment system which comes under the domain of mobile commerce system. The different types of the payment systems to be discussed in the thesis for security analysis are classified into 4 types:

1. Credit card based systems
2. Electronic checks and Account Transfers
3. Electronic cash payment systems
4. Micropayment systems

The grouping is based for the most part on the business model behind the payment solutions. The grouping may not be the best, in terms of the functional perception of the systems but it serves the purpose of presenting the different types nicely. Differences between the different groups of payment systems are not in all cases very dramatic and in many cases a real life system is hard to classify to belong to any one of the groups -for example some of the micropayment schemes could be used to implement e.g. electronic checks.
One of the prominent classes of payment found to be used in m-commerce recently is micropayment system which is based managing small payment values. Mobile payment is defined as the process of exchanging financial values between two parties using a mobile device to pay for products or services. With this new payment option, customers can pay for products and services anywhere and anytime with the comfort offered by their mobile devices. It is designed to operate with wireless technologies such as Bluetooth, Infrared or 802.11x. The electronic payment system over the wireless mobile adhoc network is one of the considerable topics of research currently. Such type of network is characterized by dynamic topology, unwanted energy consumption, and obvious link breakage. Therefore creating a dedicated and secure payment system of ubiquitous type will become a very challenging task for any researchers. From the decentralized and infrastructureless types of the network, various threats might evolved due to dynamic topology caused by random mobility of the device as well as restricted resources on trusted handheld devices. In anonymous micropayment schemes, there is no connection between the payer and the payment means. In this case, the payment means should be secured by a third party vendor which is normally any financial institutions. The financial institution should ensure the reliability and the legitimacy of each coin in the network which also means that every user who wants to verify a coin should check with the financial institution. The second type of payment is in connection to the payer, where each payment mean or token should include the characteristics of the first payer. Therefore, before accepting any payment mean, a node should substantiate the first payer and verify that he owns requires the involvement of a trusted third party. Not only this, but the payee can directly redeem the payment means or use the similar token for another payment, if the micropayment mechanism allows asking for a delegation authorization. Commercially various e-payment system are in use which works on cellular network, but the success rate is very low due to high security threats. Majority of existing transaction systems are online and are directly dependent on a fixed cellular network with increased cost for service. Such system currently in practice has no assurity of reliability and exposed a privacy infringes implicating threats to payment systems.

While electronic commerce (e-commerce) continues to have a profound impact on the global business environment, technologies and applications have begun to focus more on mobile computing
and the wireless Web. With this trend comes a new set of issues and problems specifically related to wireless e-commerce. Ultimately, researchers and developers must determine what tasks users really want to perform anytime from anywhere and decide how to ensure that information and functionality to support those tasks are readily available and easily accessible. The communications infrastructure necessary for the wireless Internet environment is quite complex. Wireless devices are likely to remain at a disadvantage over their wired counterparts in terms of bandwidth. Limited bandwidth is a significant problem that requires organizations to rethink how users interact through a wireless device with an information system. An important issue is how to create efficient applications that can realistically work with current technology. Accordingly, micropayment schemes still require the proper designing of efficient security protocols, which could become problematical according to the quantity of the payers and the environment of the payment means and payment chains. Further, this system does not describe any robust mechanisms allowing to conclude distributed payment or pay distributed applications.

### 1.5 Existing System

There have been several efforts to secure mobile payment either by migrating existing e-payment protocols for fixed networks to secure payment transactions over wireless ones [9], [17], [18] or designing new payment protocols which are specific to wireless environments [19], [15], [20], ranging from high-valued (thousands of dollars) transactions by credit-card or electronic check protocols to low-valued transactions (a few cents) by micro-payment protocols. To secure high-valued payment transactions, credit-card payment protocols, such as SET [5] and iKP [21] protocols, and electronic-check protocols [34], [35] were proposed. These protocols are based on public-key infrastructure (PKI) that are not efficiently applied to wireless networks.

To deploy PKI in a wireless environment, a client needs to perform high computational cryptographic operations, and the client’s mobile device is required to have storage for a number of public-key certificates. Moreover, during each transaction, the certificate sent to the client has to be verified by a Certificate Authority (CA) which is located in a fixed network. Although, the
pointer to the location of full certificate, typically a URL, can be used to reduce the size of certificates stored on a mobile device [22], PKI-based payment protocols still need to have additional communication passes. Alternatively, the migration of existing payment protocols for fixed networks to wireless ones was proposed by the deployments of proxy servers [23], [24], [25] and mobile agents [9], [17], [18]. We name the payment frameworks for such migration approaches as proxy-based and agent-based frameworks, respectively. In a proxy-based payment system, a proxy server located in a fixed network performs transactions on behalf of the clients. The proxy server contains all payment-related information of the clients. Thus, the clients’ storage requirement is reduced. However, the clients are required to fully trust the proxy server because their sensitive information, including private keys, is stored on the proxy server. In an agent-based payment system [9], [17], [18], a mobile agent act as a client’s assistant on performing transactions. Generally, the mobile agent is defined as a software element (program, procedure, object, thread, etc.) owned by a user. It is capable of migrating from one computer to another in order to execute a set of activities on behalf of its owner [9]. The concept of mobile agent has also been applied to mobile payment scenario in order to overcome the limitations of wireless environments, particularly to increase transaction performance [9], [18].

Several agent-based payment systems based on existing fixed-network payment protocols, mainly SET protocol [5], have been proposed [9], [17], [18]. These systems employ mobile agents to perform payment transactions on the client’s behalf. Thus, each client needs to connect to the Internet for short periods during the entire transaction. This greatly reduces connection cost for the clients. However, such systems are still susceptible to attacks due to the problem of key generation in an insecure environment [17]. To secure low-valued transactions, a number of micropayment protocols have been proposed [6], [7], [15], [8]. They deploy low computational cryptographic operations in order to minimize their operational cost compared to that of credit-card payment protocols. Applying micropayment protocols to wireless environments, most of them do not need mobile agents or proxy servers because their computational and communication load is comparatively low. We classify the payment framework for this kind of payment systems as non-proxy-based framework.
Several micropayment protocols have been proposed [8], [15], [7] based on various kinds of cryptographic operations. On one hand, PayWord [7] deploys public-key operations that have high computational load, especially at mobile users. On the other hand, symmetric-key based micropayment protocols [8], [15], which deploy symmetric-key operations and hash functions, require lower client’s computation. However, due to the nature symmetric-key operations, such micropayment protocols lack non-repudiation property [10] which is one of the most important properties for financial transactions [26]. Moreover, in order to minimize the party’s computation by reducing the number of cryptographic operations applied to the protocol, some private information, which should be known only by the appropriate parties, is transmitted in clear text during the transaction as in [8] and the assumptions of trust relationships among parties are too-strong. For example, in [15], a payment system provider knows all of its clients’ secrets. Either the lack of the non-repudiation property or the exposure of the clients’ private information allows the payment system provider to impersonate as its clients to perform payment transactions.

In any payment systems, the following transaction security properties must be satisfied [27], [15]:

- **Party Authentication**: each engaging party in the system must be able to authenticate the party whom she is communicating with.

- **Transaction Privacy**: each engaging party must be able to ensure that the messages are not revealed to any unauthorized parties, but only to the intended recipient of the messages.

- **Transaction Integrity**: each engaging party can ensure that the received messages are not altered during the transmission.

- **Non-repudiation of Transactions**: each engaging party cannot deny the transactions she has performed.

In addition to the fundamental properties described above, a secure payment system requires “Accountability” property. The accountability property is defined as the ability to show that the parties who engage in the system are responsible for the transaction related to them [26]. Generally,
accountability is considered as one of the most important security properties of e-commerce protocols since they are relevant to fund transfer and goods ordering. Each engaging party must be able to prove the association with messages sent in the protocol that she is either the originator or the intended recipient of the message.

The accountability is considered as a high-level security property which covers all the above fundamental transaction security properties. To achieve the accountability property, all transaction security properties stated above must be satisfied. Thus, the accountability property is considered as the main security property to be used for the analysis in this thesis. Several formal logics [28], [29], [26] were proposed to analyze e-commerce protocols on the accountability property. Kailar [28] proposed a logic based on belief logic [30]. Kailar’s logic does not reason about a verifier who acts as a dispute resolver [26]. Note that the reasoning about the verifier is very important because we need to state about the information that a prover can reveal to the verifier as proof evidence. Kessler et al. (KN) [29] proposed a logic which offers reasoning about the verifier’s belief. However, KN’s logic does not provide reasoning about proving without revealing secret information to the verifier. Moreover, its reasoning about hash function is too strong in that it allows the verifier to infer the input of a hash function without possessing the input itself [26].

Kungpisdan et al. (KP) [26] proposed a modification of KN’s logic for reasoning about the accountability of SET [5] and iKP [21] protocols. KP’s logic can be used to analyze e-commerce protocols which are composed of complex cryptographic messages. Moreover, it provides reasoning about the verifier and captures the provability without revealing secret information to the verifier by using a prover’s belief about the verifier’s possession of information. Normally, existing accountability logics [28], [29], [26] can provide reasoning only about the accountability of asymmetric cryptographic messages based on the assumption that symmetric cryptographic messages cannot provide the accountability because the secret key for encrypting a message is shared among engaging parties. Thus, it is not able to specify the originator of symmetric-key encrypted message. Recently, several cryptographic protocols that are based on symmetric cryptography, yet are able to identify the originator of the message, have been proposed [31], [10], [32]. Therefore,
this makes the existing accountability logics, including KP’s logic [26], not general in that they are incapable of analyzing the accountability of symmetric cryptographic messages [33]. As a result, there are several transaction performance and security issues relevant to mobile payment. The major problem still remains unsolved: the availability of practical and secure mobile payment systems.[34, 35]

1.6 Motivation

The motivation of the proposed research work is derived after analyzing the need of the research work by identifying the issues in existing system as follows:

1. The first motivation comes from the limitations of wireless environments that are primarily from mobile devices which have limited system resources and from wireless networks which have high connection cost, low bandwidth, and low reliability. In particular, a mobile user may not be able to efficiently performing highly secure transactions, which require high computational cryptographic operations, over the wireless network with the above characteristics.

2. The second motivation is related to consideration of effective routing protocols to be used in secure mobile transaction in wireless adhoc network. The situation become much worst, when mobile adhoc network is considered for mapping real time application for mobile transaction. To date, the majority of adhoc routing protocol research has been done using simulation only. One of the most motivating reasons will be to use simulation is the difficulty of creating a real implementation.

3. The third factor is the lack of sufficient security of existing mobile payment systems, mainly due to improper protocol design and the deployment of lightweight cryptographic operations which lead to the lack of important transaction security properties. Such problems have motivated the research conducted in this thesis.

4. The fourth factor identified is the lack of easily accessible and versatile standard means of mobile payments which is one of the biggest obstacles for the on-line electronic commerce
in various real time model. The systems so far have all their limitations in terms of usability and security according to the survey analysis.

5. The fifth factor exposed is the existence of unreliable protocols in electronic payment system. A large number of systems and protocols which exist already for all areas of the e-Commerce process browsing and selecting goods, ordering, paying and logistics. Probably the most in challenging of area in terms of reliability and information security, payment, is however, lacking widely accepted standard protocols and methods. This is the most important reason for the fact that B2C e-Commerce hasnt grown as quickly as possible and anticipated by many people.

6. 1. The sixth factor is identified in the area of micropayment systems are as below:

   • *Transaction Management*: It is very difficult to execute secure effective transaction methods and moreover updates in mobile adhoc networks, which is due to its sole distinctiveness e.g. lack of infrastructure, having a dynamic network topology and using resource constrained devices. Majority of the traditional research work has utilized infrastructure based m-commerce which depends on a client/server model where information is fundamentally located placed on servers within the wired network and peer nodes act as clients accessing the services provided by the servers along with an issue of service unavailability due to network disconnections. Also, the in-depth idea of a transaction can be difficult to enforce as network intermittent disconnections will affect a particular service in a secure m-commerce operations succession to fail and accordingly the secure connectivity would be considered unfinished and will be subjected to abort.

   • *Delivery of Service*: Due to the unique characteristics and complexities of an adhoc wireless network, existing service discovery and delivery protocols do not seem to suit the needs of an adhoc wireless network, making them unsuitable for m-commerce oriented scenarios. Service advertisements and deliveries may need to be disseminated by a mix of a store and forward strategy as well as local multicasting to cope with intermittent online connectivity.
\textbf{• Trust-System:} One of the important factors of online communication in terms of security will be Trust, which assists in participating entities to ensure the secure transaction by extenuating improbability and risks involved in the transactions, such as ambiguity about trading groups or entities pattern in fulfilling the transaction agreements. On the other hand, as mobile adhoc network cannot rely on a network service provider to facilitate security services such as certification authority (CA) which can assists to design trust system among peer nodes in the existing network. It can also be observed that peer nodes have to rely on their peers in the network to provide trust verification in order to evaluate other nodes fidelity. Yet, the nature of an adhoc wireless network makes trust scheme founding in this network intricate to accomplish.

### 1.7 Research Methodology

The different stages of the research methodology are listed below:

\textbf{• Gathering Information:} All the relevant information related to image extraction with emphasis on text is gathered and grouped in one place. The Literature survey to identify various prior research works pertaining to the field of interest.

\textbf{• Quantize Research Problems:} This stage includes quantizing the research issue or finding the research gap by analyzing the results of prior published work. Narrow down on to the specific problem.

\textbf{• Formal Model:} To develop a formal payment model for a practical and secure mobile payment system. The model defines characteristics and interactions among engaging parties, how the money is transferred, and important properties for a practical and secure mobile payment system.

\textbf{• Framework:} To develop a payment framework that is suitable for wireless environments. The framework not only enhances transaction performance of a payment protocol operating on it, but also provides secure transactions. In addition, the proposed framework satisfies the proposed formal model.
• *Process Oriented Architecture*: at protocol level, our objectives are shown as follows:

- Develop a secure cryptographic technique using hash chain which not only increases transaction performance while applying it to a mobile payment protocol, but the protocol also satisfies transaction security properties stated in the proposed formal model.

- Design non proxy-based payment protocols for both account-based and token-based payment transactions. The proposed protocols satisfy the proposed mobile payment model by applying the proposed cryptographic technique to them. The proposed protocols offer both secure and practical mobile payment in that:

  - They are secure in that they satisfy transaction security properties including accountability property.

  - They are practical in that they have higher transaction performance than that of existing non proxy-based payment protocols when operating on low computational capability mobile devices.

  - Not only the proposed protocols have higher transaction performance and security than existing non proxy-based mobile payment protocols, but applying them to the proposed framework also offers higher performance and security than existing mobile payment systems.

- Validate the practicability of the proposed mobile payment protocols by implementing a mobile payment system based on the proposed protocols.

- Develop a formal logic for analyzing accountability property of mobile payment protocols that is able to analyze both symmetric and asymmetric cryptographic messages. The logic can be used to analyze accountability of e-commerce protocols.

- Analyze the proposed framework and protocols primarily by using the proposed formal logic to show that a payment system based on the proposed framework or protocols satisfies the proposed model.
1.8 Research Aim and Objectives

The main aim of the research work is to investigate the root causes of security flaws in upcoming mobile commerce applications and then based on the studies; the research will aim to propose a framework ensuring secure system for designing efficient process oriented architecture for mobile transaction on wireless adhoc network.

The prime research objectives are as described below:

- To conduct thorough investigation for various security flaws in existing mobile commerce system in wireless adhoc network.

- To analyze various routing protocols in wireless adhoc network and present a design of novel hybrid routing protocols for secure and reliable mobile transaction in real time test bed.

- To design a secure m-payment system applicable in wireless adhoc network in order to secure transaction channel for the proposed algorithm implemented on it.

- To design a framework for secure micropayment system defining the inter-relationship among various constituents involved in mobile commerce system highlighting the significance of secure m-payment system in wireless network.

- To design a new verification protocol (termed as gaining algorithm) for robust authentication among client and service provider using datasets from clients android enabled handset.

- To design a novel cryptographic algorithm using SPKI and hash chaining function in order to increase multi-layer security in offline wireless adhoc network. The practical accomplishment of the algorithm aims to design the following factors:

  - The protocol must assure secure transaction characteristics along with proper authentication among various constituents involved in transaction mechanism.

  - The protocol should have optimal security in transaction in comparison to all the existing protocols or frameworks.
The approach followed for the research work are based on the following considerations:

- Majority of the previous research work have extreme deployment of expensive cryptographic protocol which is not simple to deploy as well as difficult to design the algorithms. Micro-payment systems have contributed to iterative payments from a single vendor where majority of the security policies has used one-way hash functions in order to generate a chain of hash values. Hash functions such as MD5/SHA are more computationally proficient in comparison to other symmetric key algorithms such as AES or asymmetric key algorithms such as RSA and allow for fast generation and verification of payment tokens. But maximum of the researches comes with a security loopholes and high costing. Use of advance cryptographic protocols in such cases will only increase the memory and network overhead for high requirement of maintenance of key management. So traditional cryptography cannot be deployed in securing the communication between one to another node in wireless adhoc network. The problem of reliability of communication becomes much worst when there is a frequent change in the network topology. This thesis will provide an overview of some of the relevant technologies, applications, and issues in the relatively new field of wireless adhoc based m-commerce.

- Majority of the research conducted in past and even now which is related to implementation of adhoc based routing protocols are totally simulation based, where normally the simulation being conducted using conventional simulators like NS2, OMNeT++, OPNET etc. Such types of the research will yield to analytical result which has no significance as well as clear visualization of impact of routing protocols on applications in real time environment. Just by observing graphs and animated results from NS2 based simulators, which is frequently used, we cannot definitely make out the impact of results on user experience in terms of security. The proposed research work has been totally conducted in real time using multiple atom processor, wireless networking devices, as well as smart phones with Symbian and Android Mobile OS. The thesis will reflect the original results after performing the experiments with in-depth analysis.

Majority of the research work conducted in banking process, or financial process considering the security aspect is done in online communication system. But the proposed research work has a
unique implementation of offline communication system. We also understand that one of important
issue with communication on offline in wireless adhoc network is that account permission for
client is feasible for being invalidated without vendor module knowing about it. In order to solve
this issue, the proposed system highlights account permission with very short validity duration
where bank should renew certificates frequently. Therefore if the certificate has been invalidated
or rejected by the bank, than it will be subjected for acceptance offline for a very shorter duration.
Therefore the proposed system with short term certificates has better security in the wireless mobile
adhoc network.

1.9 Scopes

The scopes and objectives of the research work are as follows:

- **Standardization**: The proposed research work is done in real time considering various hard-
  ware like Atom processor, tablet-PC, and experimented on availability of service of GPRS
  in the mobile phones, which are normally smart-phones or cellular devices with Symbian
  or Android 2.2 mobile OS. Therefore the proposed mobile payment system adheres to the
  standards frameworks defined by the WAP Forum, ITU-T, IETF, RSA Laboratories, the Na-
  tional Institute of Standards and Technology and the MeT initiative. Standards specified by
  RSA Laboratories, ITU-T and FIPS are foundation for the information security solutions in
  the system. WAP Forum and the MeT initiative define the ways in which those standards
  are applied to mobile Internet and WAP in particular. IETF RFCs form the basis for the
  networked distributed applications. The legislative framework regarding payment systems
  and their operation as well as that related to digital signing and certificates is evolving in
  Europe very quickly and probably in India very soon. New regulations and new interpre-
  tations of existing ones are being made. Defining the business models and earning logics
  for the Mobile Payment System in this regulatory and business environment would be very
  challenging.

- **Scalability**: The proposed system is highly scalable as the response times exhibited by the
  system increases linearly as the load on the system increases linearly, when not near the
maximum capacity of the system. Scalability will also means, that it is feasible to increase the capacity of the system linearly by linearly increasing the capacity of servers that host the system. There are two methods that can be used to scale up the system capacity either by increasing the number of servers running the software, or by increasing the processing capacity of each of the servers running the software. An exact measure of the scalability of the system is not defined as a criterion. Rather it is just expected that a scalable behavior be exhibited in tests run on the system.

• **Performance**: Experimentation shows that the proposed system has optimal performance. As a working hypothesis, a response time of 1 to 2 seconds for each of the services provided by the system is achieved under normal load. The performance is illustrated by running tests against the system.

• **Modularity**: The proposed system is built in such a manner, that it is possible to attach new functionality into the modules to the system, without influence to other, parallel modules as majority of the work is done in java platform. This is especially important for the interfaces towards other external systems - the interface implementations should be pluggable, i.e. re-building the entire system in order to take into operation a new interface implementation should not be necessary. Use of ready-made components or libraries is also considered in order to avoid reprogramming existing functionality.

• **Maintainability**: The proposed system is easy to manage. The systems operation is possible to follow by inspecting the system logs. The system administrator is able to correct problems by some simple means.

### 1.10 Organization of the Thesis

**Chapter-1: Introduction**

**Chapter-2: Review of Literature**

Discusses all the significant prior work that has already been benchmarked in many research work.
Chapter 1. Introduction

The prime aim of this chapter is to briefly elaborate all the prime research work with respect to cloud based mobile commerce, Mobility Aware Adhoc Network, Security insights on m-commerce in adhoc wireless network, m-payment system, Payment System on Offline Wireless Network, Process Oriented Architecture etc.

Chapter-3: Security in m-Commerce

Provides insights with various parameters, security requirements, and concepts which is required in creating a robust model for secure m-commerce system. The chapter will be also encompass various illustration for technologies for mobile payments, introduces a generic architecture for m-payments, security issues, challenges for m-payments, micro-payment systems and their analysis, and various vulnerabilities.

Chapter-4: Client verification using Gaining protocol

Introduces a framework that is based on the potential to verify the clients with trusted hand held device depending on the set of frequent events and actions to be carried out. The framework illustrated in this chapter is design after collecting a real time data sets from an android enabled hand set, which when subjected to newly introduced, gaining protocol, will result in detection of malicious behavior of illegal clients in the network.

Chapter-5: Process Oriented Architecture using Hybrid Routing

Emphasises the analysis of process oriented architecture of mobile commerce which is one of the emerging trend in mobile applications with huge demands. The chapter also presents a novel approach of process oriented architecture for secure mobile commerce framework using uniquely designed hybrid mobile adhoc routing protocols using reactive and proactive type in real time test-bed.

Chapter-6: Process oriented Structural Design using Hash Chain

Incorporates a process oriented structural design for securing m-payment system using hash chain and Simple Public Key Infrastructure that is implemented on newly designed digital agreement of broker along with paving new secure routing for secure m-transaction as an efficient alternative for
digital coin. The chapter also presents a novel approach of designing highly secured and robust process oriented architecture for micropayment system in wireless adhoc network. Deployment of any confidential transaction over dynamic nature of wireless adhoc network will strike a high amount of security challenges which is very difficult to identify which poses a great difficulty in designing and effective countermeasures.

**Chapter-7: Conclusion**

A brief summary of the research work carried out is given along with a critical evaluation, major contributions and scope for future research. Each chapter has a section In Retrospect, summarizing the chapter content and a list of published papers arising out of that chapter.