ISSN No. 0976-5697

Volume 4, No. 10, September-October 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhancing Personal Identification Number (Pin) Mechanism To Provide Non-Repudiation Through Use Of Timestamps In Mobile Payment Systems

Dr. Joseph Wafula Muliaro
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
Nairobi, Kenya
muliaro@yahoo.com

Isaac Kega Mwangi*
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
Nairobi, Kenya
isaackegs@gmail.com

Dr. Stephen Kimani(Phd)
Institute of Computer Science and Information technology
Jomo Kenyatta University of Agriculture and Technology
Nairobi, Kenya
stephenkimani@googlemail.com

Abstract: Personal identification mechanism (PIN) is a widely used mechanism especially in applications dealing with financial transactions. It is widely used due to its easy way of implementation in that it's as easy to implement PIN mechanism as it is easy to employ passwords in the application; also it is easy for the users to remember a 4 digit number that remembering a password. For these and other more reasons PIN is the mostly used mechanism to authorize transactions in a payment application, but due to its advantages PIN has never been able to provide non-repudiation. Non-repudiation is defined as the act of ensuring that parties that are involved in a transaction do not fault on that transaction. It acts as a evidence that indeed a said transaction took place between a set of parties and either of those parties cannot fault on that transaction. Hence the main goal or objective of this project was to enhance PIN to provide non-repudiation through the use of timestamps. Timestamps are one of the mechanisms that can be used to provide non-repudiation in applications.

Keywords: PIN(Personal Identification Number), Non-repudiation, Time-stamp .Pin-Timestamp Algorithm, Non-Repudiation of Origin (NRO), Non-Repudiation of Receipt (NRR)**,** Non-Repudiation of Submission (NRS)**,** Non-Repudiation of Transport (NRT).

I. INTRODUCTION

Mobile payments, also known as m-payments, may be defined as any payment where a mobile device is used to initiate, authorize and confirm an exchange of currency in return for goods and services. Mobile devices include mobile phones, PDAs, wireless tablets and other devices that can connect to mobile telecommunication networks. Mobile payments can be an alternative to cash, checks, credit cards and debit cards, and can make possible new opportunities for commerce convenience [1].

Most mobile payment systems use the Personal Identification Number mechanism as an authorization mechanism. This mechanism makes use of numbers keyed in by the registered users to authorize a transaction. One aspect of PIN that has not been fully tackled is for it to provide non-repudiation [2].

Hence in the light of this shortfall, this research paper proposes to enhance PIN to provide non-repudiation through the use of timestamps. The outcome at the end shall be a proposed algorithm called the PIN-Timestamp algorithm that shall seek to enhance Pin to provide non-repudiation.

II. LITERATURE REVIEW

Mobile payment is a new and rapidly adopting alternative payment method – especially in Asia, Africa and Europe [3]. Instead of paying with cash, cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services and digital or hard goods such as:

a. Music, videos, ringtones, online game subscription or items, wallpapers and other digital goods.
b. Transportation fare (bus, subway or train), parking meters and other services
c. Books, magazines, tickets and other hard goods.

The two most widely used standards for m-payment applications are Global System for Mobile communications (GSM) and Code Division Multiple Access (CDMA). GSM based phones use a SIM (Subscriber Identification Module) card which is a detachable smart card containing the user's subscription key used to identify a user. In CDMA based phones, the phone itself stores the subscription key [4]

The most common mobile payment technologies are

a. Premium SMS/USSD: **Unstructured Supplementary Service Data** (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network. USSD messages are up to 182 alphanumeric characters in length. Unlike Short Message Service (SMS) messages, USSD messages create a real-time connection during a USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS. The consumer sends a

payment request via an SMS text message or an USSD to a short code and a premium charge is applied to their phone bill or their mobile wallet. The merchant involved is informed of the payment success and can then release the paid for goods. [5]

b. Contact Less Near Field Connectivity: Near Field Communication (NFC) is used mostly in paying for purchases made in physical stores or transportation services. A consumer using a special mobile phone equipped with a smartcard waves his/her phone near a reader module. Most transactions do not require authentication, but some require authentication using PIN, before transaction is completed. The payment could be deducted from pre-paid account or charged to mobile or bank account directly. Mobile payment method via NFC faces significant challenges for wide and fast adoption, while some phone manufacturers and banks are enthusiastic, due to lack of supporting infrastructure, complex ecosystem of stakeholders, and standards [3].

A. Mobile payment system types:

M-payment systems are of two types - Remote Payments Systems and Proximity payment Systems. In the former, the payer and the payee are at remote locations, e.g. a customer places an order from his home to a retail store. In the latter, payer and payee are in the same vicinity, e.g. a customer (payer) buys a cup of coffee from a vending machine (payee). As shown in Figure 3, the following steps are typically involved in carrying out a transaction using a Remote m-payment system [4]

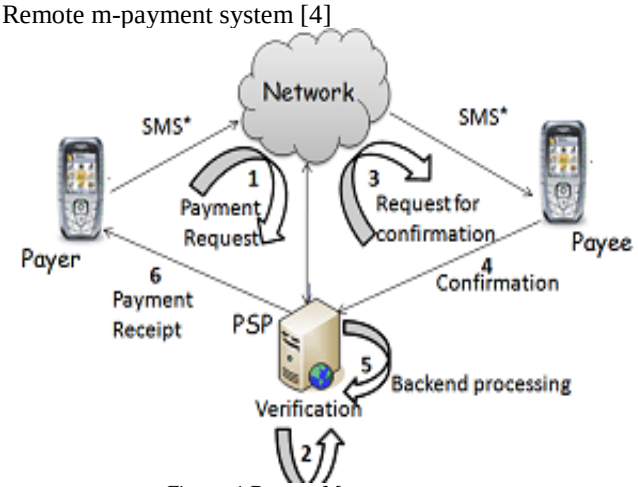

Figure: 1 Remote M-payment system

a. The customer uses his mobile device to send a payment request to a PSP (payment service provider) over a wireless network. This request includes the details of the payee and amount to be paid.
b. A PSP (payment service provider) verifies the credentials of the customer and the payee (basically it checks whether the customer and payee have registered for such an m-payment service). Optionally, the PSP might ask the customer for some more details (like a password) for authentication.
c. Once the credentials of the customer have been established, the PSP requests the payee for confirmation by forwarding the payment details.
d. The payee then sends a confirmation message to the PSP.
e. After successful confirmation, the PSP performs backend processing to update the accounts of the payer and the payee.
f. It sends a payment receipt to the payer. It might also optionally send a "Transaction completed" message to the payee.

The transaction processing in proximity m-payment systems is similar to the process followed in remote m-payment systems. The main difference lies in steps 1 and step 3. In remote m-payments, the customer first sends the payment request to the PSP over a wireless network by using a remote wireless technology. The PSP then forwards this request to the payee. However, in proximity m-payments, the customer directly sends the payment request to the payee typically using a short-range wireless technology. The payee then forwards this payment request to the PSP over a wireless network [4].

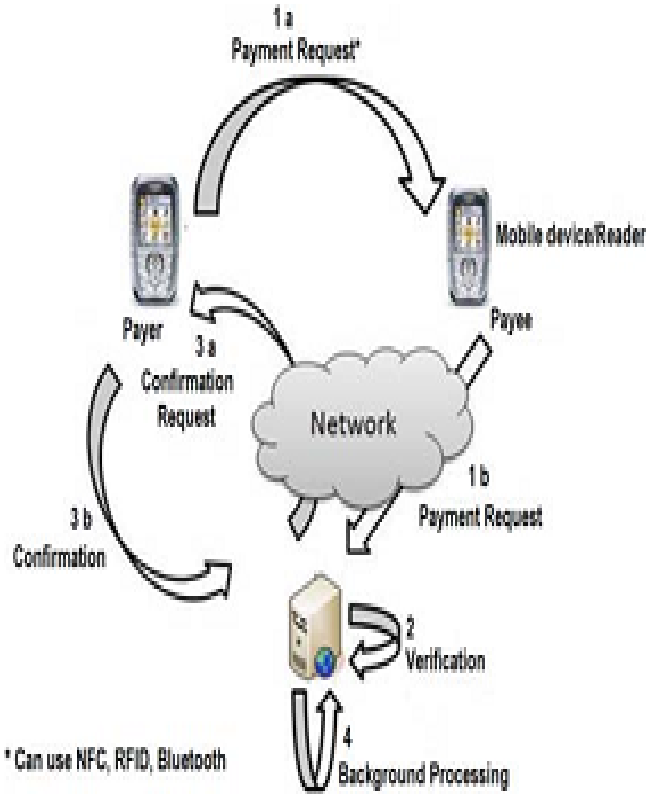

Figure 2: Proximity m-payment system

Apart from this classification m- payments can also be categorized based on the payment value involved (Micro, and Macro payments) and the charging method used (Post-paid, Pre-paid, and Pay-now) [4].

B. Security Issues In M-payment Systems:

M-payment system rides on some underlying infrastructure (say GSM) or employs a technology (like Bluetooth or RFID). The security vulnerabilities in such underlying technologies are often ignored while analyzing the security aspects of an m-payment system. An accurate security analysis is possible only if we take a holistic view of the vulnerabilities at each dimension instead of considering only a specific dimension (say protocol or platform) of the m-payment system. First we have to consider the layers of support for m-payment systems as shown below [4]:

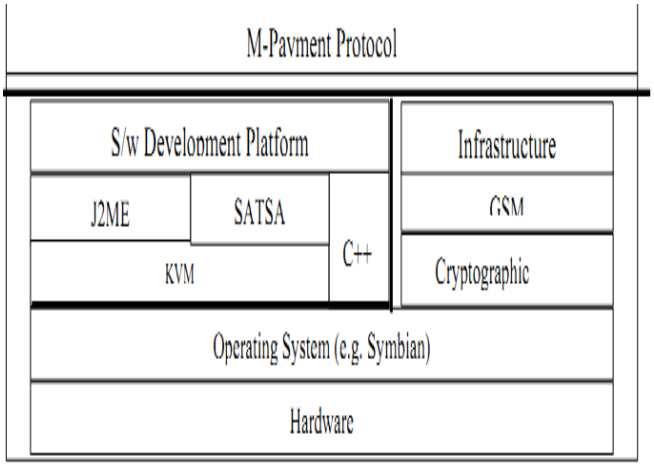

Figure 3: Layers of Support for m-payment

At the highest level we have the m-payment protocol which rides on top of a software development platform and a wireless infrastructure. These underlying components in turn have a layered architecture comprising APIs, Operating Systems, and hardware. The KVM (K Virtual Machine) is a compact, portable Java virtual machine intended for small, resource-constrained devices such as cellular phones. To ensure the security of the m-payment system as a whole it is necessary that every layer in the m-payment system is free from attacks like man-in-the-middle attack, replay attacks or impersonation attacks. Security features like authentication, authorization, confidentiality and non-repudiation are an absolute necessity for any m-payment application. The designers of the m-payment application may choose to derive some of these features from the underlying layers. Based on the above discussion, we now create taxonomy of some of vulnerabilities at different layers and their effects. We briefly describe these vulnerabilities and examine how existing or proposed m-payment systems they could affect.

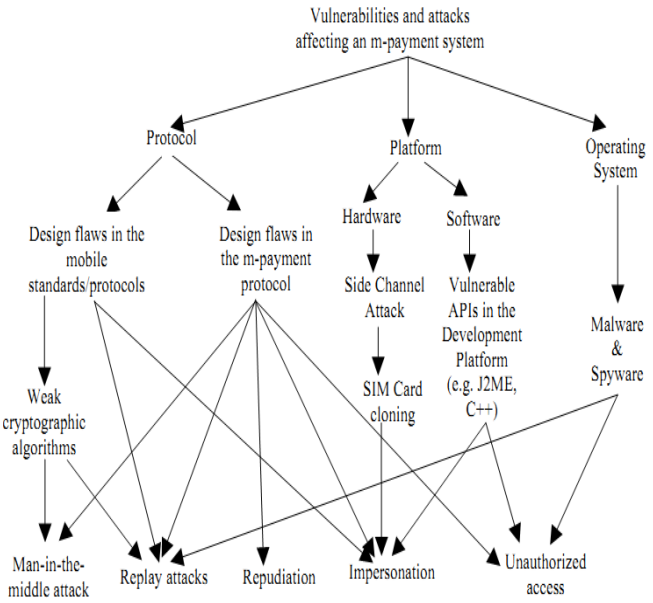

Figure: 4

a. Vulnerabilities in GSM:

One option in m-payment system design is to leverage the existing mobile network infrastructure since it already has authentication and encryption mechanisms in place. Before doing so, a security analysis of the currently used mobile standards is necessary. 2G GSM uses A5/1 and A5/2 stream ciphers for encrypting data so that over-the-air communication privacy can be ensured. The design of both these algorithms was kept secret. However, it became public knowledge through reverse engineering and it was demonstrated [6] that A5/1 and A5/2 do not provide an adequate level of security. However, 3G mobile communications uses a block cipher, A5/3 that is much stronger as compared to A5/1 and A5/2. Some attacks on 2G GSM protocols were published in [6]. These attacks include a cipher text only attack on A5/2 that requires few milliseconds of encrypted on the air conversation for finding the correct key in less than a second on a computer. On networks using A5/1 and A5/3, these attacks are more complex. For these networks a man-in-the-middle attack can be launched whereby an attacker impersonates a base station to the user.

b. Vulnerabilities due to the way of implementing the application on the chosen platform (Case study: J2ME) :

No matter how safe and secure an m-payment scheme is, it could still be insecure due to the security vulnerabilities in the platform chosen for implementing the scheme. As mentioned in the previous section, J2ME is one of the preferred platforms. Several researchers have developed prototypes for their m-payment systems using J2ME. Debbai, Saleh, Talhi & Zhioua documents vulnerability in some Java- enabled phones that can be exploited to write a malicious MIDlet that sends SMS messages without requiring the user's authorization. This could affect the security of some SMS based schemes that require the user to send a SMS message (to the payment gateway) to initiate a transaction. If a malicious MIDlet were installed on the user's phone that sends SMS messages then it would be possible to initiate a transaction without the approval of the user. Thus need for an authorization constraint that can ensure that only authorized transactions are transacted at the payment gateway [7].

c. Vulnerabilities due to the choice of technology (Case study: Bluetooth):

The vulnerabilities in the technologies employed such as Bluetooth and RFID can severely compromise the security of a proximity payment scheme. Several attacks have been proposed on the Bluetooth protocol in the past. Most of these attacks are either theoretical in nature or are possible due to a bug in the implementation (and not because of a bug in the protocol itself) [8]. For example, Bluetooth air sniffers make it possible to sniff the raw data being exchanged between two devices. Access to this data could open several possibilities for an attacker such as cracking the PIN. Cracking the link key can launch a form of man-in-the-middle attack. Such attacks could have a serious impact on the security of m-payment schemes. In practice, it would be a bit farfetched to expect a hacker to purchase expensive Bluetooth air sniffers but then again a hacker might find it worth making an investment considering the monetary gains that he could make by breaking into an m-payment scheme [9].

C. Authorization And Non-Repudiation:

a. Authroization:

Auth orization (also spelt **Authorisation**) is the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular [10]

b. Mechanisms used for authorization:

The following are some of the mechanisms that can be employed in payment authorization:

a) ***Digital signatures****:* Digital signatures can ensure the authenticity of transaction parties, integrity, and non-repudiation of transmissions. A digital signature is created when the document to be transmitted is enciphered using a private key. The process of enciphering the document using the private key authenticates the document, since the document could only have been enciphered using the private key of the owner. A digitally signed document or message is unalterable after the signature. The recipients can verify the signature by deciphering using the public key. In real world, documents are not completely encrypted to save time. In such cases one-way hash functions are used [11].

b) ***Personal Identification Number (PIN) authorization****:* PIN has to be entered by the user to authorize any operation that needs authorization from either party. PINs are most often used for automated teller machines (ATMs) but are increasingly used at the point of sale, for debit cards and credit cards [12].

c) ***Biometric authorization:*** This is where for an authorization to be allowed, a person usually can use either one of his/her body parts usually the eyes or fingers to authorize the transaction. The biometric signature of the person is stored in a database usually at the mobile operators servers from where if they want to transact they just put the part needed and the transaction is completed [13].

D. Non-Repudiation:

Non-repudiation refers to a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement or contract. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated" [14].

a. Non-Repudiation Services:

Non-repudiation service can be separated into non-repudiation of origin (NRO), non-repudiation of submission (NRS), non-repudiation of transport (NRT), and non-repudiation of delivery (NRD). NRO is a combination of non-repudiation of creation and non-repudiation of sending, and NRD must be seen as catenation of non-repudiation of receipt (NRR) and non-repudiation of knowledge services are explained below:

a) Non-Repudiation of Origin (NRO):

The NRO service provides the recipient of data with proof that protects against any attempt by the sender to falsely deny sending the data. The evidence (non-repudiation of origin token, NROT) is generated by the originator of the message and sent to the intended recipient. The originator sends both the message and the NROT to the recipient. To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window [15].

b) Non-Repudiation of Receipt (NRR):

The NRR service provides the sender of data with proof that protects against any attempt by the recipient to falsely deny having received the data. The evidence (non-repudiation of receipt token, NRRT) is generated by the recipient of the message and sent to the originator.

The recipient sends both the reply message (if any) and the NRRT to the originator. To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window [15].

c) Non-Repudiation of Submission (NRS):

The NRS service provides the sender of data (that may be another DA) with proof that protects against any attempt by the DA to falsely deny having accepted the data for transmission. The DA *does not care* what the content of the message is. The originator (or a preceding DA) has sent a message to the (next) DA that receives this message and sends the NRS token to the originator (or the preceding DA establishing a chain of intermediate NRST tokens providing chained NRS).

To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window [15].

d) Non-Repudiation of Transport (NRT):

The NRT service provides the sender of data with proof that protects against any attempt by the DA to falsely deny having delivered the data to the intended recipient. The DA *does not care* what the content of the message is and *cannot guarantee* that the message is duly received by the recipient. The evidence (non-repudiation of transport token, NRTT) is generated by the DA delivering the message to the intended recipient (the last DA in the chain of DAs) and send back to the originator. To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window [15].

b. Mechanisms for providing non-repudiation:

Non-repudiation mechanisms providing evidence should be based upon cryptographic techniques using symmetric or asymmetric techniques as described by ISO/IEC13888-2 or ISO/IEC13888-3, respectively [15].

The application of asymmetric techniques (using digital signatures) is recommended and requires the involvement of an off-line TTP (Trusted third parties) to guarantee the genuineness of keys (public key certificates management including CRLs and directory servers).

Symmetric techniques (using secure envelopes) MAY be applied instead and REQUIRE an on-line TTP for generation and validation of the secure envelopes including resolution of origin preventing fraudulent repudiation (mechanisms using shared secret keys does not allow a distinction to be made between the parties sharing the key, and thus – in contrast to digital signatures – does not provide NRO). The mechanisms have to provide protocols for the exchange of non-repudiation tokens specific to each kind of

non-repudiation. These tokens MAY be stored as information by disputing parties for arbitrage [16].

The non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. For evidence generation, the TTP MAY act on behalf of a principal involved in as token generation authority (TGA), digital signature generating authority (DSGA), time stamping authority (TSA), notary authority (NA), and monitoring authority (MA). Evidence transfer MAY be carried out by a TTP acting as delivery authority (DA) or evidence record-keeping authority (ERA). At last, the TTP MAY be in the role of an evidence verification authority (EVA). The above is based on the use of asymmetric techniques of non-repudiation [17].

E. Secure Time-Stamps:

A **time-stamp** is a sequence of characters, denoting the date or time at which a certain event occurred. In modern usage it usually refers to data stored in a computer or digital electronic equipment. In many cases, the difference may be inconsequential: the time at which an event is recorded by a timestamp (e.g., entered into a log file) should be very, very close to the time of the occurrence of the event recorded. This data is usually presented in a consistent format, allowing for easy comparison of two different records and tracking progress over time; the practice of recording timestamps in a consistent manner along with the actual data is called **time-stamping**. Timestamps are typically used for logging events or in a sequence of events (SOE), in which case each event in the log or SOE is marked with a timestamp. In file systems, timestamp may mean the stored date/time of creation or modification of a file [18].

a. Time stamping Schemes:

There are many time-stamping schemes with different security goals, and these schemes are [18]:

a) (Public Key Infrastructure) PKI-based - Timestamp token is protected using PKI digital signature.
b) Linking-based schemes - timestamps is generated such a way that it is related to other timestamps.
c) Distributed schemes - timestamp is generated in cooperation of multiple parties.
d) Transient key scheme - variant of PKI with short-living signing keys.
e) MAC - simple secret key based scheme, found in ANSI ASC X9.95 Standard.
f) Database - Document hashes are stored in trusted archive; there is online lookup service for verification.
g) Hybrid schemes - Linked and Signed Method is prevailing.

The most common type of time-stamping technique used in the PKI-based Timestamp. The technique is based on digital signatures and hash functions. First a hash is calculated from the data. A hash is a sort of digital fingerprint of the original data: a string of bits that is different for each set of data. If the original data is changed, then this will result in a completely different hash. This hash is sent to the TSA. The TSA concatenates a timestamp to the hash and calculates the hash of this concatenation. This hash is in turn digitally signed with the private key of the TSA (Time Stamping Authority) . This signed hash + the timestamp is sent back to the requester of the timestamp who stores these with the original data Since the original data cannot be calculated from the hash (because the hash function is a one way function), the TSA never gets to see the original data, which allows the use of this method for confidential data [18].

a) Checking the timestamp:

Checking correctness of a timestamp generated by a time stamping authority (TSA).

Anyone trusting the time-stamper can then verify that the document was not created after the date that the time-stamper vouches. It can also no longer be repudiated that the requester of the timestamp was in possession of the original data at the time given by the timestamp. To prove this the hash of the original data is calculated, the timestamp given by the TSA is appended to it and the hash of the result of this concatenation is calculated, call this hash A. Then the digital signature of the TSA needs to be validated. This can be done by checking that the signed hash provided by the TSA was indeed signed with their private key by digital signature verification. The hash A is compared with the hash B inside the signed TSA message to confirm they are equal, proving that the timestamp and message is unaltered and was issued by the TSA. If not, then either the timestamp was altered or the timestamp was not issued by the TSA [18].

III. RESULTS AND DISCUSSION

A. Motivation Statement:

The growth of the mobile industry has greatly increased the trading efficiency in our country whereby most people prefer to transfer cash through their mobile phones than by physically carrying the cash around. This provides security for the person, also enables a person to transact even from the comfort of his/her own home. But with this comes the challenge of repudiation. Most traders have been cheated by scrupulous customers or even other traders whereby they agree to trade and when it comes to committing the payment, the other party faults on the deal. Thus in the light of this many traders still prefer to transact with hard cash with their customers.

Most mobile operators have put in strict measures to ensure that their services are not used by criminals or people who have other agendas in mind apart from following the correct procedures while effecting payments. The mobile service providers usually flag suspect transactions and can even go a step ahead and bar the person from using their service or even take up legal action against the suspect. There are also several mechanisms the service providers use to ensure that they protect their clients against repudiation cases like ensuring that there is atomicity of their transactions. But in the light of all these efforts being done the service providers, the aspect of enhancing PIN to provide non-repudiation has not being successfully tackled.

In this paper, an algorithm is being proposed to enhance personal identification number mechanism to provide non-repudiation through use of timestamps. This algorithm in the end shall be implemented in a prototype of a mobile payment application using SMS to send payment requests to the application. In light of this I wish to stress that this project was in now way trying to come up with a new mobile payment application but simply to enhance the current authorization mechanism which is the personal

identification number to provide non-repudiation. Also the project does not deal with the aspect of registering users for the service because the aspect of assigning PIN numbers to the users has not been tackled in this project.

IV. PROPOSED DESIGN

The main design requirement of this project was to deduce an algorithm that will enhance PIN to provide non-repudiation through use of timestamps. The algorithm which was deduced has three integral items that must be captured for it to be effective and these are the PIN that shall be entered by the clients to authorize a transaction, the numbers of those involved in the transaction and the system time. The reason for this is to cater for the most important categories of non-repudiation which are NRO (Non-repudiation of origin), NRR (Non-repudiation of receive), NRS (Non-repudiation of submit) as described which are the major repudiation services as stated by ISO specification [15]. The design of this aspect shall be divided into:

a. The algorithm
b. System model of the proposed prototype

A. *Proposed Pin-timestamp algorithm:*

Algorithm PIN Time stamp Generation (PIN, Payer number, payee number, System Time)

NRO AND NRR services represented in steps 1 to 7 of the algorithm

Step1: Define SIZE: (size of the PIN length)
Step2: Find numbers of payer and payee.
Step3: Check numbers if they are registered for the service in the database
Step 4: if (Payer number and Payee number= Stored Numbers)
They are registered for the service
Else Terminate request
Step 4: Count Number of Characters of the PIN (Integer)
Step 5: Is it the correct PIN
Step 6: if (Count = Size) and PIN=Stored PIN
Correct Input and ready for authorization of transaction
Else return Wrong PIN;

Step 7: Date/Time of Transaction is sought through use of the system time of the machine running the application.

NRT service represented from step 8 to 11 of the algorithm

Step 8: Transaction Id, Date/Time, Payer and Payee numbers, amount and PIN are counter checked before request is committed and stored temporarily in the in_msg table.
Step 9: The Payer and Payee numbers, Transaction Id, amount and Date/Time of transaction being stored as in the out-msg table.
Step 10: Send message with confirmation of the payment request

This algorithm starts by checking the numbers of those involved in the transaction, if they are registered or they are in the users database then the algorithm allows for the next step in the payment request to go ahead which is the payee's PIN is checked. If either one of the parties is not registered for the service then the request is terminated and an error message sent to the parties involved.

The timestamp is generated by the system time of the machine running the application. In implementing the algorithm it was deemed necessary to have the numbers of those involved in the transaction because most of the repudiation cases occur with people who are not registered for the service.

B. *System model of the proposed application:*

a. Use case diagram

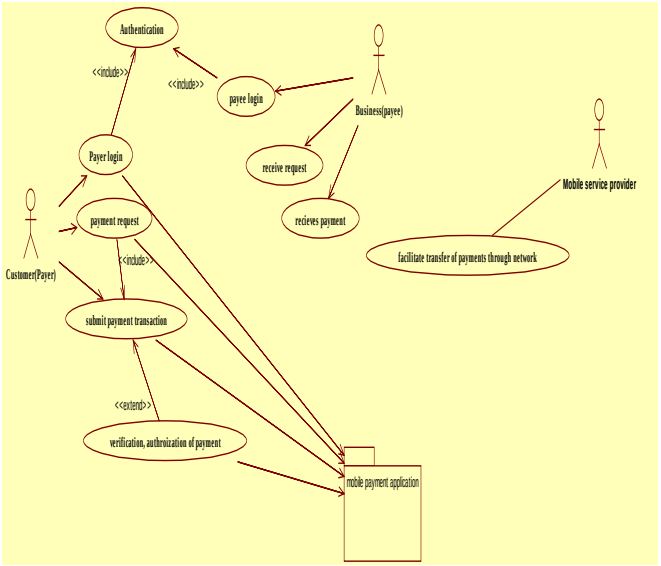

Figure 5: use case diagram

The figure above is a use case diagram for the proposed system. The figure above was constructed through the use of the star UML software based on Simon Fong's approach [20]. The use case diagram usually helps in denoting what the various entities in the proposed will be, what their actions shall be, whom they shall interact with. The above diagram contains the main characteristics found in a class diagram namely

a. ***Actors:*** these are usually roles played by a user in the proposed system. in the above figure the actors are:
a) ***Customer(payee):*** this is the person who usually is concerned with making the payment
b) ***Business:*** actor entails the person receiving the payment from the customer
c) ***Mobile network operator:*** provides the GSM network infrastructure that shall be necessary in the transfer/sending of the payment messages from the client to the mobile payment application and then in turn from the mobile payment application to the merchant's phone.

In the above use case diagram, both the client and the merchant have the same functionality in that they can both do payment request, withdraw, query account status from their handsets

b. *Use cases:* depict externally required functionality: the use cases involved here are the Payer login which shall be done when the user access their mobile phone, typing in the payment request and submitting the payment request, checking the PIN

in the payment request and authorizing the request if the PIN is correct. Also the other use cases like receiving and facilitating the transfer of the request to the mobile payment application are also shown in the diagram

C. Sequence Diagram:

This is graphical representation of system objects on time flows and the connections between the flows. The vertical dashed line is called the objects lifeline and it represents the objects life during the entire interaction. Each message is represented by an arrow between the life lines of two objects. The objects are shown as boxes at the top of the dashed vertical line

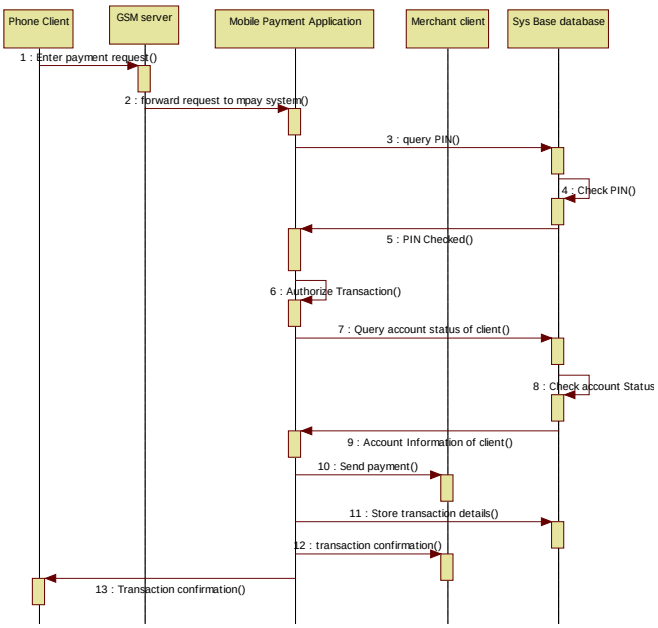

Figure 6: Sequence diagram showing the flow of information

In figure 6 above we see clearly the objects that have been defined as the:

- ***a. Client mobile:*** in this object the client uses a mobile phone to initiate a mobile money transafer between themselves an the merchant. The client writes an sms which is specified in a special format to differenitiate it from other sms as a payment sms. He/she then sends the sms that shall be routed via the GSM network or the sms gateway application that shall be used to emulate the GSM network. The message or activity here is send sms with amount, merchant mobile number and PIN code to authorize transaction.
- ***b. GSM/SMS gateway:*** this object represnts the mobile network infrastructure that is responsible for sending and receiving of messages between the client and the merchant. It is responsible for channeling the message to the mobile payment system.
- ***c. Mobile Payment application:*** It is responsible for accepting the payment request, validating the PIN entered and authorizing the transaction if the PIN entered is the correct PIN. It is also responsible for displaying authorization and confirmation of transaction messages to both the client and the merchant if all goes well with the transaction. It is also resposible for crediting and debiting the accounts of the merchant and the client respectively.
- ***d. Merchant:*** this object represents a person who is involved in the tranasction with the client. The merchant recieves the confirmation message stating that funds in their accounts have been credited after the transaction. This message acts as proof of reciept by the merchant of the funds. For the merchant to withdraw this money he shall have to go to an agent of the mobile service provider or financial institution that implements this application so that he can be able to withdrwa and get hard currency.
- ***e. Sys Base:*** it is the database that shall be used to store the applications information. The database shall hold the PIN of the clients, their account balances and status of the transactions that are being done. The database shall act as the repository for the transactions being done by the applications.

The client also recieves a similar message stating that funds have been transferred from their account to the merchants account thus acting as evidence that the transction was done and that the correct person received the money.

In this proposed application it is important to state that all these transactions are virtual in that a person has to access a withdrawing point either from the financial institution side or the mobile service providers in order to get hard currency.

D. Class Diagram:

Figure below shows the class diagram for the proposed mobile payment application. The class diagram contains the major class which is the GSM Form Payment request; this class is the major class that shall be used in doing the payment request for the client and merchants. The merchant query and client query classes are used by the GSM form payment request to query the account status of the merchant and client, this is necessary because a transaction will not be effected if the account is below the transfer amount. The phone client and merchant client classes contain the details of both the merchants and the clients. Here when authorizing a transaction the GSM form payment request shall check the PIN in these classes in order to ensure that only the correct PIN is used to authorize the transaction.

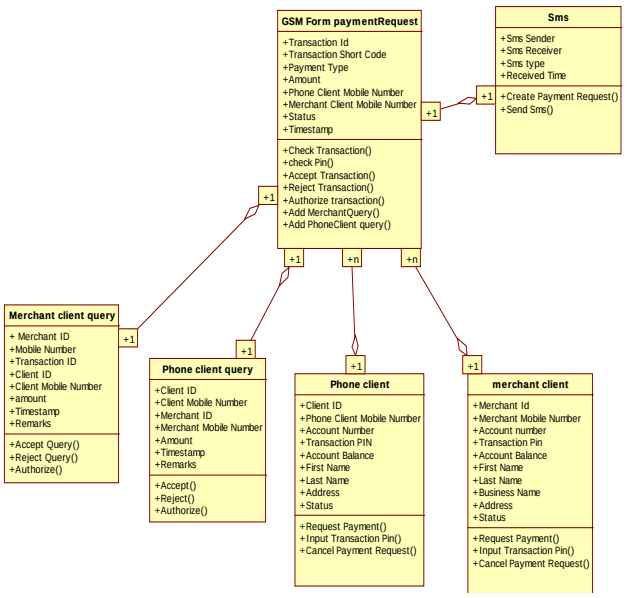

Figure 7: Class diagram

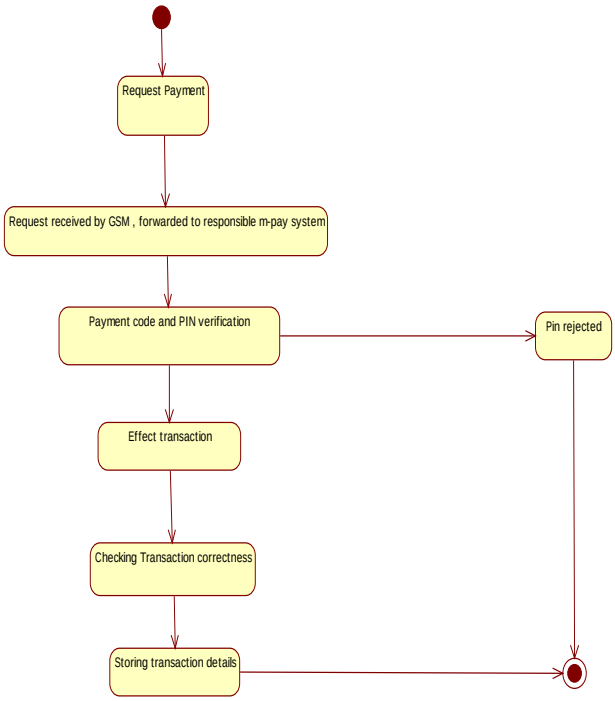

Figure: 8 State Diagram

This diagram above helps in describing the behaviour of the system. it will help in showing all the possible states a particular object can get into and how the object's state wll change as a result of events that reach the object. Hence figure 4 shows clearly how a user makes a payment transfer to another user through use of the propsed mobile payment application. As shown the first state is whereby the user makes a payment request by inputng his PIN code, amount, number of the merchant and sends the SMS. The request is received by the SMS server which forwards it to the mobile Payment application for processing. Here the application checks both numbers invloved in the transction(both for the client and the merchant), the account balances of the two, checks the PIN inputed by the client to authorize the payment. If the PIN inputed is correct, the transaction is authorized and the transfer of funds is effected. The application ensures that the transction is correct and then completes the transaction. The details that is theconfirmation messages are sent to both sets involved in the transaction. The transaction logs are stored in the database. The logs stored in the database contain the transaction id, time the transaction was done, the PIN, senders and recievers numbers and the amount of the transaction.

V. EXPERIMENTATION AND EVALUATION

A. Goal of conducting the experiment:

The Main goal of doing the experiment was to ascertain whether implementing personal identification number (PIN) with timestamps would enhance the capability of the PIN mechanism to provide non-repudiation services.

B. Equipment involved in doing the Experiment:

a. For this experiment to succeed properly, it was deemed necessary to experiment the proposed system using a real mobile device instead of using emulators or mobile test tools. The reason for this is that emulators lack the real limitations being provided for by the use of real mobile devices. That is the limitation exposed by the use of real devices is lacking in emulators, thus the test done on an emulator may function but when you transfer it to a real device and the limitations come into play the approach may not work at all [19].

b. A modem will also be needed as this will help in relaying the payment request to the application for processing.

c. A SIM card that shall be used with the modem which shall aid in relying the payment request to the mobile payment application [20].

d. A laptop to run the proposed application. The laptop shall also have the SMS gateway that shall help in relaying the payment request to the application for processing and also do the confirmation messages to both sets involved in the transaction.

C. Running the developed application:

After successful setup of the application, it is run to see whether it would achieve the main objective and that was to enhance PIN with timestamps to ensure non-repudiation capabilities of the Personal Identification Number mechanism that shall be used to authorize transactions in the proposed approach. In the proposed application there are four components involved.

The users had to send a pre-formatted SMS that shall aid the mobile payment application to process the request. The format of the SMS is given <B, W, T, D> # <Number>#<Amount>#<PIN>

Where:

a. Codes for <B, W, T, D>
   - B: Code for checking the balance
   - W: Code for withdrawing money from the account
   - T: Code for transferring money to the intended recipient.
   - D: Code for depositing money into the clients account

b. Mobile number: Number of the intended recipient whom the transfer is being transacted to their account.

c. Amount: amount that is being transacted

d. PIN: PIN number that shall be used to authorize the transaction.

Break down of the elements used in the proposed mobile payment application.

a) Phone Client and Merchant client: represent mobile devices that emulate the basic functionalities of a mobile client and a merchant client acting as a wireless payment device. The client will need to authorize the transaction before the request is accepted by the mobile payment application while the merchant client will receive confirmation of the payment request from the client through the mobile payment application. Both will receive confirmation messages when the transaction has been completed detailing the time it was done, amount transferred, account balances and name of the person involved in the transaction.

b) SMS Server emulates the background functionalities of the GSM server employed by

mobile network operators. The server basically receives the payment request from the client or merchant and forwards the message to the application for processing. Thereby after processing, it will again ensure that the confirmation messages are relayed to the prospective parties. The SMS server utilizes the modem and the SIM card inside the modem, from which respective forwarding of the messages will be carried out through the SIM card in the modem [20]. In this case a SIM card belonging to the YU mobile operator was used.

c) The proposed mobile payment application will receive the payment request forwarded by the SMS server, check the PIN and authorize the transaction if the PIN is correct. The application will also ensure that the transaction details are stored in the secure repository or database.

d) Database that shall store the transactions being done. It shall also store the PIN numbers of the clients, hence when authorizing the transactions; the application will check the PIN number that was entered by the user against the one that was stored in the database.

Basically the phone client and merchant phone client emulate the basic functionalities of the mobile device being used as an electronic payment tool. The account of the phone client will be credited of the amount while that of the merchant will be debited of the same amount that the phone client requested to make a transaction of. The results of the transaction will be stored in the database.

D. Results Of The Experiment:

The purpose of this experiment was to see whether non-repudiation could be provided for in the Personal Identification Number mechanism (PIN). From the proposed algorithm discussed in the system design, the aspect of implementing PIN with timestamps was tested in the application.

a. The first aspect of security was whether the system could authorize payments based on the PIN number being entered. It checked the PIN number provided for in the SMS with the one stored in the database for that client.

b. The pin which the user provided was checked against the one stored in the database.

c. During the checking of the Pin, another aspect was being formulated in the background because with every payment system the time aspect is every important, thus the system was to record the time the request for payment was made. This time is based on the system time of the machine on which the application is running. The time is recorded in the database.

d. Thirdly was to check whether the applications repository offered a secure storage for the transaction details.

e. The capturing of both PIN, and the time at which the transaction was being done was also checked. This helped in checking the atomicity of the transactions based on real time of the system.

f. The application contains an out-message table which holds the messages that have been processed by the application.

g. The database also contains an in-message table which holds the incoming payment request. Immediately the request is received, it is forwarded for processing after which the message isn't stored because the application will keep on processing the request.

The objective was achieved because in the algorithm proposed in the design phase, sought to use both these mechanism which work independently of each other but the algorithm sought to have them work hand in hand to enhance non-repudiation in PIN The algorithm was formulated to find a way to enhance PIN with timestamps. In most application these two are implemented separately but the algorithm sought to have them implemented together where after the mobile numbers of the parties had been verified the PIN was checked and thereafter a timestamp generated that would indicate the time the request was sent. After the request was processed, the details pertaining to the transactions would be sent via sms to both parties and the details of those messages stored in the out_msg table and the accounts of those involved are debited and credited respectively.

The algorithm when implemented had to cater for other information that is necessary in applications that deal with money transfer such as the details of those involved in the transaction and the amount.

The algorithm further had to check whether those in the request were registered to use the service. If either of the parties was not registered the request would not be processed. For the request to be processed both parties had to be registered and the one doing the transfer had to enter the correct PIN to authorize the transaction.

E. Screen shots of some of the system Runs:

a. Database screenshot of the out-message table:

This table contains all the messages that after the request have been processed by the mobile payment application. As shown the table contains the time column, here the timestamp is implemented that shows the time the request was committed and the number to which the amount was transferred. Depending on whatever action the user choose, it will be captured in this database.

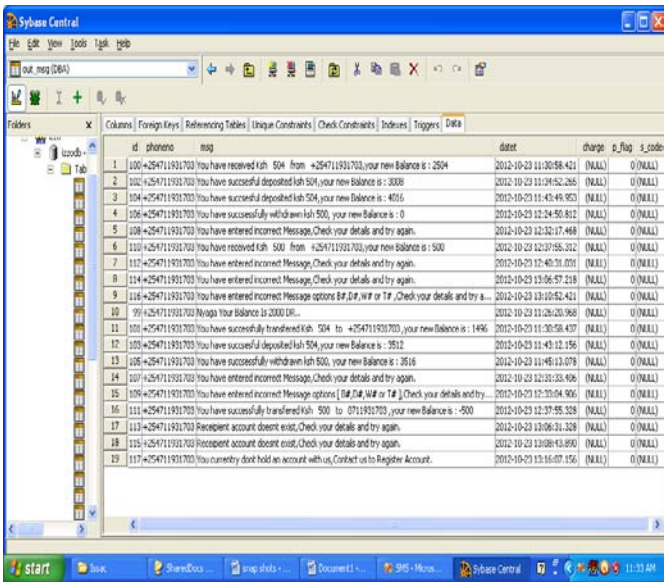

Figure 9: Out_message table of the database

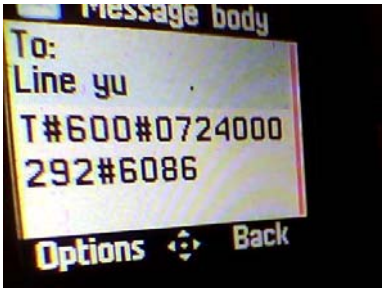

Figure 10: Screenshots of a request to transfer 600 shillings to a user number 072400292

b. Transferring Money between buyer and seller:

The screenshots above shows a transaction between two parties. In the figure above the sender sends a message to the SIM card in the modem (Line yu) which will in turn reroute it to the payment application because it is in the preformatted text which signifies that it is a payment request. The payment request is to transfer 600 to a person whose number is 072400292. Upon verification of the request as was said in the algorithm, if the said numbers are in deeded registered to use the service then the payment is effected which is a shown below with the successful completion of the request. As shown in the screen shots below. The funds will be credited and debited respectively.

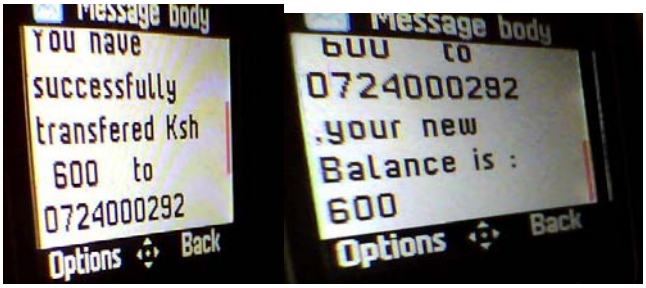

Figure 11: screenshot of a successful payment request to transfer funds

VI. CONCLUSION

a. From the algorithm one aspect that is shown is that it combines both the PIN entered by the user, time the request was submitted, number of the parties involved in the transaction. Most applications that are involved in the payment business tend to have these mechanisms separate. The PIN mechanism is implemented by itself, so as is the timestamp mechanism. The proposed algorithm helped in combining the two mechanisms together, the PIN first is checked and if it is either correct or wrong a timestamp is generated for that request and depending on the outcome of the checking of the PIN the request can either be accepted or rejected. If rejected a message is sent to the party alerting them on the error that has occurred which shall then be stored in the out_msg table in the database. The time being used by the algorithm is being issued by the system, which is the system time which is used as the TSA (Time Stamping Authority) in the application. The details of the two are stored temporarily in the in_msg table in the database. These details are deleted after processing of the request to help in curtailing the application from repeating the same transaction over and over again.

b. Another aspect of the algorithm is that it combines the four non-repudiation plans together which are NRR, NRT, NRS, and NRO. These are very important aspects of non-repudiation which should be implemented in any application to ensure that repudiation does not occur. NRR and NRO are the most important of these 4 and the algorithm caters for them. In NRO the algorithm takes the PIN entered by the person sending the request, amount, recipient's number and time stamped using the system time. The NRR takes the amount sent, the sending party and the time the request was committed. The proposed algorithm caters for the two non-repudiation plans in the scheme at once. Even if the request was not accepted still the log will be saved in the out_msg table with all the details pertaining to the request except the information on the PIN which is secretive.

c. Due to the checking of the numbers involved in the transaction by the algorithm in the database, it ensures that only registered users to the service are allowed to transact. In case an unregistered person tries to use the service, the request will not be processed.

A. Business Benefits:

One aspect of the proposed application is that it gives the developer the freedom to implement both timestamps and Pin mechanism together, thus making the development of such applications to be less costly than before.

A business benefit to a business owner is that they are able to transact with the customers he/she feels free to transact with, also this application ensures that only registered persons can use the application to transact. This will reduce the fraud cases that are being done through other mobile payment applications.

VII. REFERENCES

[1]. T. Dahlberg et al., (2007). Past, present and future of mobile payments research: A literature review, Electronic Commerce Research and Applications, doi:10.1016/j.elerap.2007.02.001

[2]. Kuhn, D. R., Hu, V. C., Polk, W. T., & Chang, S. J. *Introduction to public key technology and the federal PKI infrastructure.*. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD. 2001 (Pg 8)

[3]. Funk, J. L."The future of the mobile phone Internet: an analysis of technological trajectories and lead users in the Japanese market". Vol. 27 (1). 2005. Technology in Society, (Pg 69-83)

[4]. Agarwal, S., Khapra, M., Menezes, B., & Uchat, N. Security Issues in Mobile Payment Systems. *Indian Institute of Technology, Bombay, India*. 2007. (Pg 2)

[5]. Wikipedia, Unstructured Supplementary Service Data.

http://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data.html

[6]. Barkan, E. Biham, E. Keller, N. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. Vol 21 (3). JOURNAL OF CRYPTOLOGY. 2008 (Pg392-429)

[7]. Debbai, M. Saleh, M. Talhi and C. Zhioua. Security analysis of mobile Java. Proceedings of Sixteenth International Workshop on Database and Expert Systems Applications. 2005, (Pg 231- 235).

[8]. D. Kugler.. Man in the Middle Attacks on Bluetooth. In Financial Cryptography. Vol '03, Long Beach. Lecture Notes in Computer Science, Springer-Verlag. 2003.

[9]. L. Carettoni, C. Merloni and S. Zanero. Studying Bluetooth Malware Propagation: The BlueBag Project. Vol. 5, (2). IEEE Security &Privacy. 2007

[10]. Wikipedia, Authorization.

http://en.wikipedia.org/wiki/Authorization.html

[11]. Wikipedia, Digital Signature mechanism.

http://en.wikipedia.org/wiki/Digital_signature.html

[12]. Wikipedia, Personal Identification Number mechanism.

http://en.wikipedia.org/wiki/Personal_identification_number.html

[13]. Wikipedia, Biometric authorization.

http://en.wikipedia.org/wiki/Biometric_authroization.html

[14]. International Organization for Standardization, ISO Standards ISO/IEC 13888-1:2009, Information technology-Security Techniques-Non-Repudiation- Part 1: General Introduction http://www.iso.org

[15]. International Organization for Standardization, ISO Standards ISO/IEC 13888-2:2009, Information technology-Security Techniques-Non-Repudiation- Part 2: Mechanisms using symmetric techniques http://www.iso.org

[16]. International Organization for Standardization, ISO Standards ISO/IEC 13888-3:2009, Information technology-Security Techniques-Non-Repudiation- Part 3: Mechanisms using asymmetric techniques http://www.iso.org

[17]. Wikipedia Trusted Time Stamping.

http://en.wikipedia.org/wiki/Trusted_timestamping.html

[18]. Keynote, White Paper on "Testing Strategies and Tactics for mobile Applications".

http://www.keynote.com/docs/whitepaper/WP_Testing_Strategies.pdf

[19]. S. Fong and E. Lai. “Mobile Mini-payment Scheme Using SMS-Credit”. International Conference on Computational Science and Its Applications-ICCSA. 2005 pp. 1106-1114.

