Architecture of a Mediation System for Mobile Payment

Boutahar Jaouad
EHTP,B.P 8108, Oasis,
Casablanca, Morocco

El Hillali Wadii
EHTP,B.P 8108, Oasis,
Casablanca, Morocco

El Ghazi El Houssaïni Souhaïl
EHTP,B.P 8108, Oasis,
Casablanca, Morocco

***Abstract*—Nowadays, the mobile phone has become an indispensable part of our daily. Exceeding the role of a communication apparatus, and benefitting from the evolution of technology, it could be used for several uses other than telephony, energy of photography, the geolocation, until the control of the health condition and the quality of the air, by measuring the cardiac pulsations, the temperature and the ambient content water. In this context, financial institutions wishing to take advantage of this wave of technological change and taking advantage of the telecom infrastructure robust and secure existing began to innovate to offer a new range of payment services based on mobile phone. Thus, in this article we present a proposal for an implementation of a mediation system of payment per mobile based on the technology of the Webservices.**

Keywords—M-paiement; M-Commerce; Android; Webservices; NFC; RFid

I. INTRODUCTION

Mobile technology knew a very strong evolution in the last decade, reserved at the beginning only with one privileged class, today the mobile phone is with the range of everyone[23,24,25]. International Telecommunication Union [1], estimates that in 2014 the mobile number of subscriptions will exceed the world population (Figure 1), in at the beginning of 2014 mobile number of subscriptions already reached 6.8 billion, that is to say a penetration rate of 93%. In the first quarter 2013, they are 425,8 million the number of mobile phones sold in the world, in rise of 0,7% compared with the sales of the first quarter 2012 [2].

The mobile phone exceeded the role of an apparatus of communication, the financial institutions wanted to benefit from the infrastructure telecom already present, to offer new banking services via the mobile. This started with the transfer of money per mobile, intended primarily for the countries in the process of development, allowing the people not having an bank account to carry out transfers of money per mobile, in addition a new concept saw the day, called the mobile banking or "Any where any time banking", the bank in the vicinity making it possible to have the whole of the banking services offered by an agency via the mobile phone [3].

Also, with the growth of the sector telecom, of new technologies appeared, in particular the Internet on mobile with the 3G, the 4G, Wi-Fi Outdoor, and soon the WIMAX….

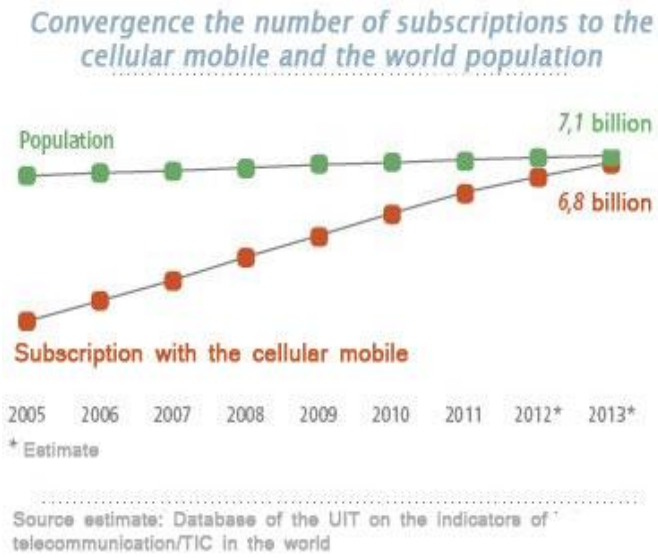

Fig. 1. Convergence of the number of subscriptions to the cellular mobile and of the world population

That supported the expansion of Smartphones. According to [4] the sales of Smartphones exceed those of the ordinary portables, thus exploding of 46,5% over one year, between April and June 2013, it was sold in the world more than 225 million Smartphones against 153 million one year earlier.

Vis-a-vis this revolution of mobile technology, a new form of purchase was born, the Mobile Commerce. The mobile phone became, thus, a system of payment offering a very high level technologies of safety compared to the traditional banking purchasing card [5], the manufacturers do not cease offering new means of safety such as the reading of the digital fingerprint or the recognition of the face of the owner, or technology NFC (NEAR Field Communication), allowing the payment without contact.

The banking main actors, in particular Visa, estimate that in the next years the mobile phone will replace the bank card, as means of payment, especially in the countries in the process of development. The bank card remains a means very vulnerable to the frauds, according to [6] the amount of the frauds with the bank card reached 1,55 billion euros in 19 European countries in 2013.

The service providers and the banks start to invest in the mobility solutions, by offering new services of payment per mobile, the use remains very limited, compared to the potential of this equipment. The service providers propose gravitational mobility solutions, but they are always based on the bank card like support of payment. Other shares the solutions suggested by the banks are only restricted with their customers, as these services are often limited to the payment of invoices (Electricity, Water, Telephone …).

After the comprehensive study of current systems of payment we propose to set up a central system of mediation based on the technology of Web services, allowing the customers to centralize the payment of the services of the suppliers to which it is adhered. For example the customer, will have the possibility to pay his invoices (Water, Electricity, Telephony.) in only one operation instead of going (the customer) on each site of the supplier. This operation will be carried out by the customer through a Mobile application (face-End), which will communicate with the Back-End part of the mediation platform.

A Mediation system makes it possible to have a uniform access for heterogeneous and distributed data sources. Figure 2., illustrates the general architecture of mediation systems, made up of a whole of data sources wrapped as a data source XML, and connected has a total interface (Integated Global View). Thus, the customer communicates with only one total data source instead of communicating with each base of give independently. The interfaces provide a uniform syntax of communication with the whole of the databases.

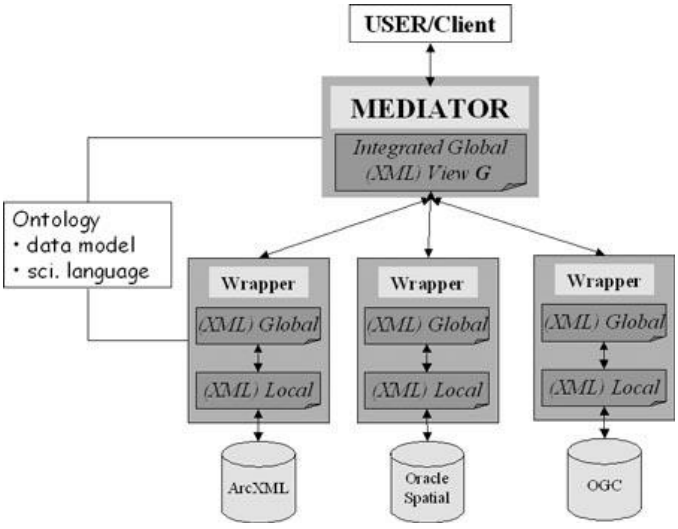

Fig. 2. Extended mediator architecture - Source: GEON: Toward a Cyber infrastructure for the Geosciences—A Prototype for Geologic Map Integration via Domain Ontologies

To give confidence to the client and the provider in our system, the operation of mediation is completely transparent to them, the platform leverages web services already offered by providers, the treatment is carried out at the platform at the time of client connection, it recovers in a single operation, all services payable by connecting to each supplier information system, after the confirmation of the customer, the platform is responsible for validating the payment to suppliers.

II. Related Works

Research on the architectures of mobile payment systems have inspired many researchers until today, it would be difficult to group the literature as a specific disciplines. Further evidence of this can be seen in the fact that the articles on mobile commerce and mobile payment are scattered across various journals in disciplines such as business, management, marketing, engineering, technology information (IT) and information systems (IS) [26].

The evolution of research on this field and reciprocal to that of mobile technology in the last decade with the advent of mobile searches have focused on the architecture of the payment systems and money transfer via mobile among researchers who are interested in this we find Jerry & Krishnaveni [17] (1), Ashutosh & Manik [27] (2).

(1) Jerry & Krishnaveni [17] propose a system of money transfer P2P-based mobile phone, set up a protocol for communication between the seller and the buyer, so they have developed a security strategy system implementation.

(2) Ashutosh & Manik [27] propose an architecture for mobile payments, to replace the credit card information by saving the EMV card chip on the SIM card.

On the other hand, and with the advent of the internet, and taking advantage of the implementation of the GPS system on the mobile phone, searches were interested in mobile commerce, in addition to the use of mobile phones as a means of replacing the credit card payment, a new layer is added to the purchase on the mobile.

Currently research is focused on contactless payment via NFC technology, this research found among those of Rahul & Shubham [28] propose to set up a platform for mobile payments based on NFC technology.

The common thread among most of the research is that they are always based on the existing banking network to make the payment or transfer of money, and they all focus on the payment interface part, the work that pluparts we met do not address the payment transaction from start to finish but they are only limited to the replacement of the card by the mobile phone.

III. Description of the Platform of Payment

The mobile operating systems were very well evolved; this made it possible to the merchants to propose richer and gravitational portable applications. Currently the majority of the merchants offer portable applications containing in addition to one window of the products, of the more relevant functionalities (points of fidelity, accounts - checks gifts, the geolocation and comparators of the prices…), this tendency is called the Mobile commerce, and it is regarded as an evolution E-commerce [7].

In addition, the customer thus finds himself vis-a-vis a whole of mobile applications installed on his smartphone, it is thus constrained to be identified with connection on each one of these applications, also for each operation of payment / purchase, it needs to obtain the information of his bank card, for example, for the payment of the invoices of electricity and

of water, the customer is obliged to pay with that bank card for each service, knowing that comes from only one supplier. The operation of payment a remains complicated, and presents a risk of safety, one can say that until now, the applications of payment or purchase per mobile only of the E-commerce are not encapsulated in an portable application not exploiting the potential of the mobile phone, also, they are restricted to the people having a credit card.

To be more open, easier and more made safe, we set up a mediation system based on Web services allowing to centralize the proposed services by the suppliers and to ensure the payment of these services. The platform is connected automatically to the information system of the suppliers to recover the whole of the services to which the customer is registered, offering the possibility to the customer, in only one operation the payment of the whole of its services. The platform offers to its customers a virtual account containing his balance, enabling him to pay these services. That offers the advantage to the customers not having an bank account to also exploit the services of the platform. The platform is connected via channels of communication with the traditional systems of payment (interbank networks, systems of transfer of money) making it possible its customers to reload their virtual accounts. In addition the platform offers to the customers having an bank account to store encrypted information of the bank card in the data base of the platform, thus, and for safety reasons, the customer does not need more to seize them for each operation of payment, the platform as an intermediary, will undertake to restore this information in a protected way.

The main advantages of the platform rest on the following aspects:

*1) F*acility of use:

- Facility of adhesion (Customer/Supplier).
- Ease of payment.
- Dematerialization of the invoices paper in those electronic.

2) Opening:

- The platform does not suggest any restriction for adhesion.
- The platform makes it possible any supplier to propose the payment of its services to its customers.
- The platform is connected to all the interfaces of traditional payment.

3) Made safe:

- The platform respects the international security standards in particular the PA-DSS.

A. *Use of the platform*

The customer with the possibility of exploiting the services of the platform via two channels:

1) Via a Mobile application:

The customer with the possibility of exploiting the services of the platform on its mobile phone, in particular the creation of the account, the payment of the invoices of its services, the notification of the invoices.

2) Via an E-commerce website :

The platform can be useful like channel of payment on the E-commerce website of the merchant, that the customer can choose at the time of the payment, thus the customer can choose to pay is by virtual account or of its credit card via the platform.

B. *Component of the platform*

The platform consists of three essential layers (Figure 3):

1) The mobile customer: a multiOs portable application installed on the customer smartphone allowing exploiting the services of the platform.

2) The mediation system: a central server playing the part of offering federator of services proposed by the providers of the services exploitable by the customer and the suppliers. Having interfaces of communication with the traditional networks of payment. In addition to the operations of payment, the platform must be able simultaneously to deal with the communication with the various heterogeneous information systems from the suppliers and to be able to treat and to synthesize their various structures.

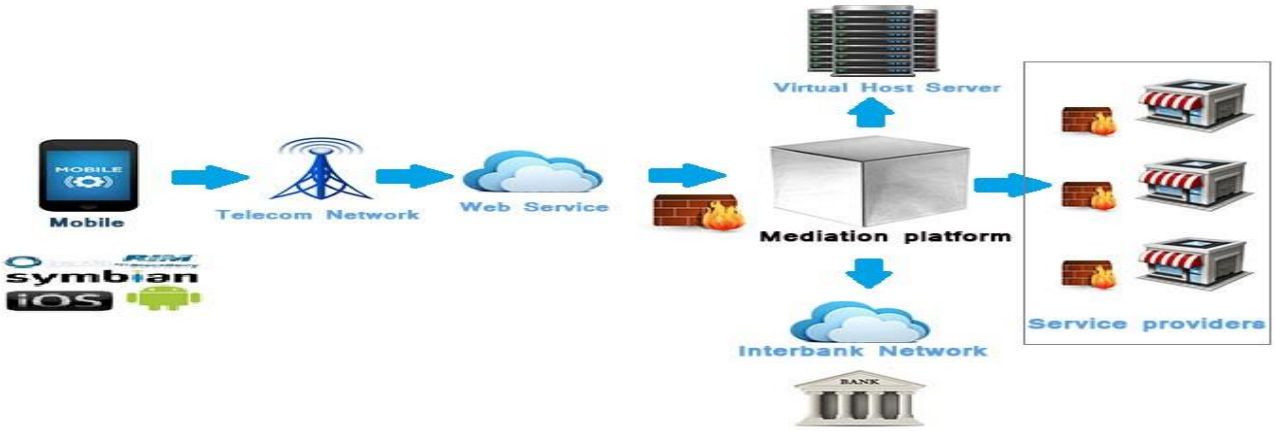

Fig. 3. Global description of the mediation platform

3) Partners: the principal partners of the platform are the suppliers of the traditional services (Electricity, Water, Telephones, Internet, Taxes ...), these partners are connected to the platform via adapters.

C. Description of the platform services

1) Creation of the account user:

To be able to exploit the platform services, the customer starts by creating an account by seizing his personal informations via the mobile application, the administrator of the platform validates the creation of the account, a virtual account is created automatically in the Host Server "Virtual Host Server" containing information of the balance of the platform customers, the account user is identified by a Single code UIC "**Unique Identifier of the Client**", it will be the support of principal payment of the user.

Once connected by the mobile application, the customer starts by choosing the list of the services for which he wishes to adhere, an authentication near the supplier is required to validate the adhesion of the customer to the service. The platform automatically retrieves all services payable on suppliers from the user login, the customer also receives a notification from the presence of an invoice for a service to be set.

2) Reload Virtual account:

During the creation of the account user, the platform offers to the customer to reload his virtual account by:

- Credit card: The customer with the possibility of reloading his virtual account by using its bank card, via interfaces of the platform with the interbank network.
- Transfer of money: the platform is connected to partners of transfer of money via Web services, making it possible to feed the virtual account of the customer in real-time at the time of a transfer operation of money.

3) Recording of the banking informations:

We designed our platform so that it is independent of the banking sector to allow people without bank accounts to access payment services via their mobile. The interface with the banking or money transfer structures is useful only to reload the customer's virtual account, if not all payment transactions will go through the virtual account platform. Storage of credit card information is only option offered by the platform for customers to use the platform as a means of payment instead of entering their data on the website of traders because of security.

In accordance with the PA-DSS, the information from the credit card (BIN, CSC, expiration date of the card) is encrypted before being stored in the database, for against it shall store the PIN . When a payment transaction, the customer can choose the payment channel or through virtual account or by bank account. If paying by credit card, the platform decrypts data and validates the payment.

IV. Platform Architecture

Among the great difficulties of taking into account in the installation of a payment system is the response time, especially for the systems connected to the interbank network. The leaders of the electronic money impose an optimal response time for the treatment of the transaction, VISA for example obliges a response time less than 10 seconds if not the transaction will be rejected by a answer code ''TIME OUT'' (BFFF0015) [8], to respect the banking standards, the architecture of our mediation system of payments will be built in two levels :

- "**Front office**" part: During the validation of the payment by the customer, this part takes care of the checking of the balance customer, confirmation of payment to suppliers, the payment and the generation and the recording of the journal of the transactions in the platform database, and the emission of a receipt to the customer.
- "**Back Office**" part: This part takes care of the consolidation operations between the platform and the suppliers; this concept is inspired from the banking environment called operations of clearing, allowing the interbank consolidation [9]. These operations are generally done in end-of-day in order to not occupy the performances of the production servers; it acts to generate the reports/ratios of accountancy while being based on transactions journals. These reports/ratios will be the support of suppliers payment starting from the clients' account.

A. Description of the Components of the platform

The mediation system platform respects a modular architecture, where its components are independent and communicate between them (Figure 4).

The interface "**Mobile Interface**" is charged to treat all the requests of the customer by mobile, the request for connection passes by this interface, by calling the module "**Authentication**" this module starts by authenticating the customer by basing on this information stored in the database "**Account Customer**", after the authentication of the customer, this module checks via the module "**Access Control**" the services to which the customer has the right to reach, this module recovers the rights of the customer while being based on information of the database "**Platform services**".

Once connected, the customer with the possibility of listing the invoices to pay via the module "**Service Management**". This module carries out a connection to the unit of the services to which the customer is registered to recover the invoices automatically to be paid. This with the advantage of avoiding with the customer explicit connection to the platform of each supplier to pay his invoices, but the platform centralizes the whole of these subscriptions, the communication with the suppliers passes via the interface "**Partner Gateway**" by using the Web services technology.

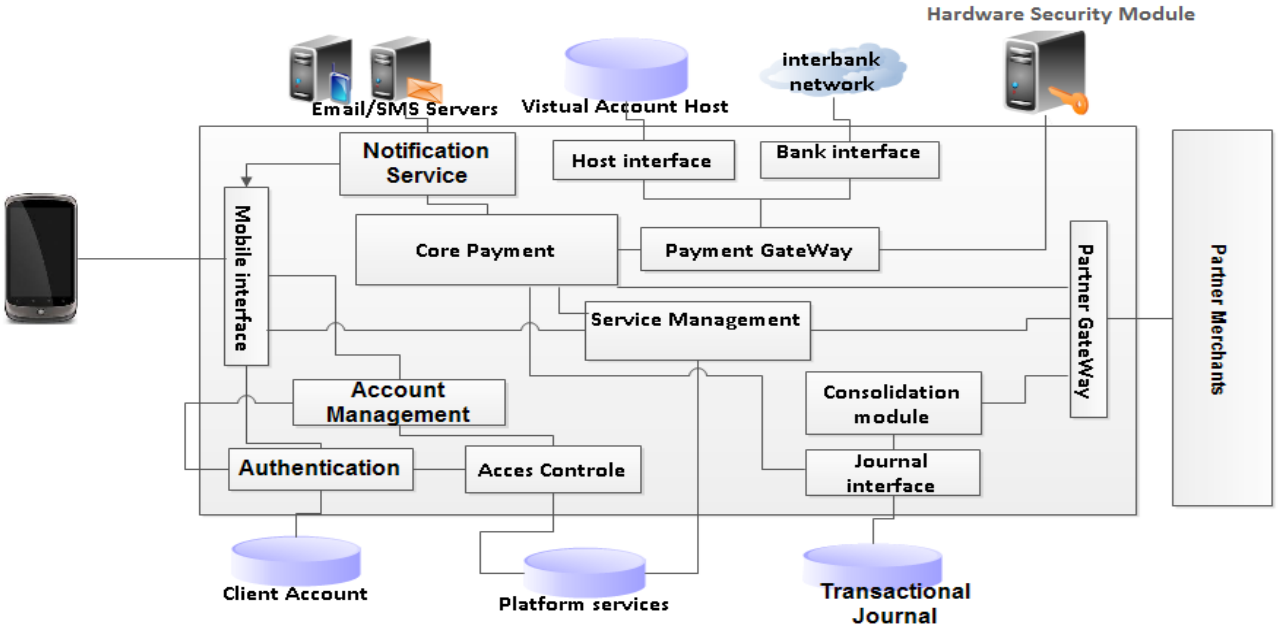

Fig. 4. The platform architecture.

The customer selects the list of the invoices to be paid and validates his payment, the module "**Service Management**" calls upon the module of payment "**Core Payment**" this unit deals with the operation of payment, it starts by calculating the amount of the transaction, and proposes to the customer the interface of payment wished via the module "**Payment Gateway**", if the customer chooses his credit card as payment medium, this last will pass by the interbank network via the interface "**Bank interfaces**", if not the amount of the transaction is debited from the customer' virtual account "**Virtual Account Host**" via the interface "**Host interfaces**".

The module "**Core payment**" validates the payment with the supplier and records the report of the payment transaction in the database "**Transactional Journal**" via the module "**Journal Interfaces**", once the report of the transaction recorded the module "**Core Payment**" informs the customer of the result of the transaction via the module of notifications "**Notification Service**" by SMS and transmits to the customer email address the electronic invoice.

The module "**Consolidation Interfaces**" takes care of the generation of the reports of the whole of the operations of day laborers payment generated via the platform while basing itself on information of the base "**Transactional Journal**", this information will be used like support of compensation thereafter.

V. THE PLATFORM MODELING

The platform modelling is carried out in two parts:

A. *The first part:*

The first part concern the mobile customer, it describes the whole of the functionalities suggested for the customer via the mobile (Figure 5) and which can be gathered in four essential modules:

1) The inscription at the platform: This module gathers the whole of the functionalities of inscription at the platform, starting by seizing these personal informations, the choice of the services and the methods of payment, this information will be transmitted to the administrator for the final validation of the creation of the account.

2) The account Management: This module covers the whole of the spots of administration of the account to knowing the consultation of the balance of the virtual account, the food of the virtual account by (transfer/Bank card), the personal modification of information, also it makes it possible to the customer to safeguard information of its bank card (the PIN code, the CSC, and it scratch date).

3) The suppliers/services Management: This module allows the management of the services suppliers partners of the platform, it makes it possible to the customers to adhere to the the various services suppliers.

4) The management of the services: This module takes care primarily of the payment of the services, it recovers the list of the services to which the customer is registered, it is connected to the suppliers servers to recover the services to be regulated, it also makes it possible automatically to notify the customer of the presence of the possible services to be regulated.

B. *The second part:*

The second part relates to the mediation platform (Figure 6), the modeling of this part is structured in three parts:

1) Implements customer services: This part covers the implementation of the Web services invoked by the customer via the mobile application, and which are the list of the services, the management of the account the inscription at the platform, the management of the services.

Implements customer services

2) Administration of the platform: This part covers the functionalities suggested with the administrator of the platform being an actor of the platform; these functionalities set out again in three parts which are, the management of the customers in particular the validation of the creation of the account, the management of the suppliers, and the follow-up of the transactions.

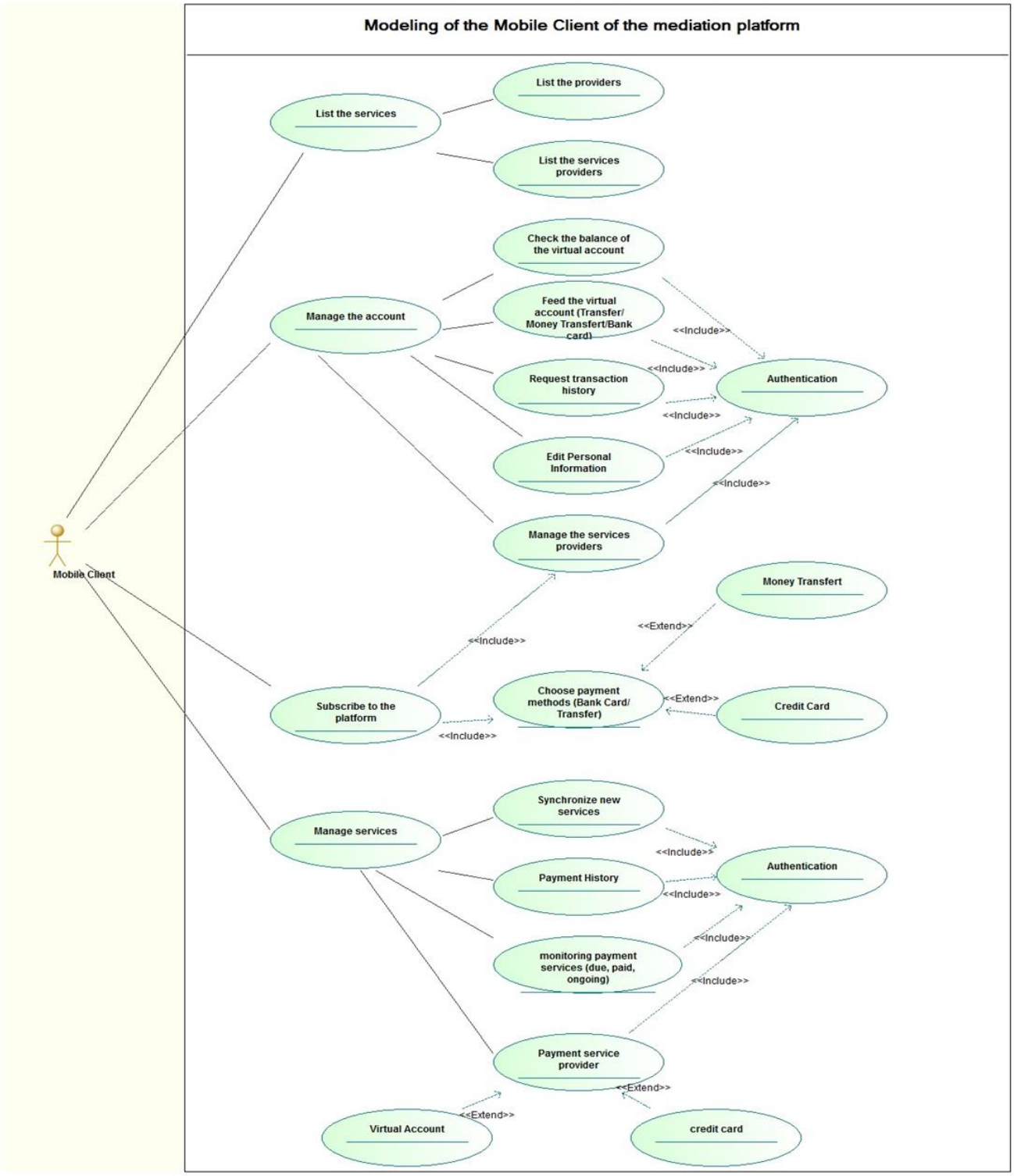

Fig. 5. Uses cases of Mobile application part.

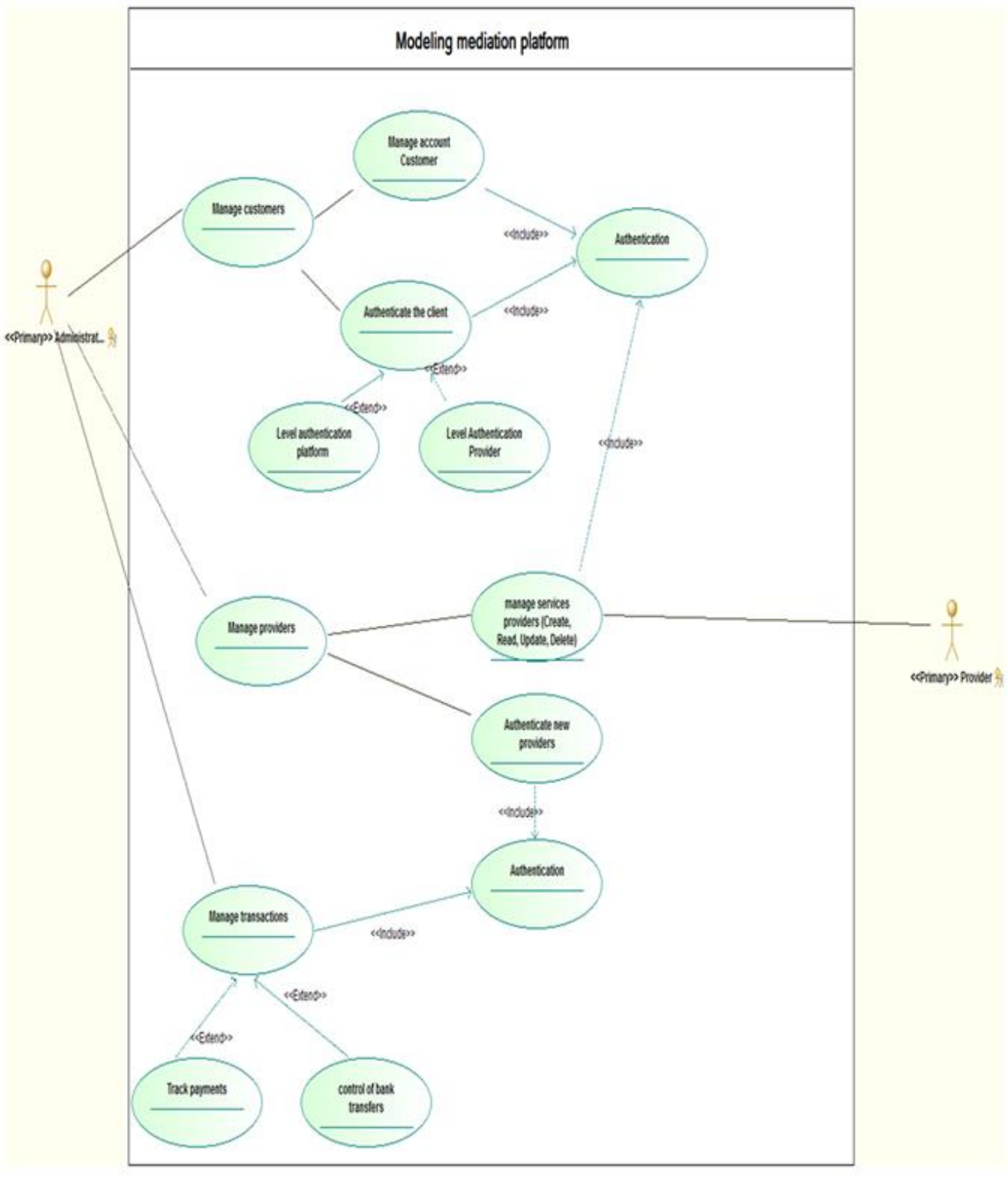

Fig. 6. Platform Uses cases.

VI. TECHNOLOGIES

A. The Mobile custome

To be able to cover a great mass of customers, the customer should be accessible via all mobile technologies.

We noted a very relevant point at the time of the choice of the mobile technology, which is mobile Frameworks of development, such as PhoneGap [10], and jQuery Mobile [11], and of others, generally based well on technologies HTML5, and JQuery, they implement the notions of the MDA (Model Driven Architecture) for the automatic generation of the source code, this starts by creating the model of the application, Framework is automatically given the responsability to generate the source code of the application for the whole of the operating systems mobile (Android, IOS, RIM, Windows Mobile…), this with the advantage of reducing considerably the time of development of mobile applications, also this reduces the complexity of development. One is obliged to have forcing of competences on all the Mobile computer programming languages.

In addition, we noted that these Frameworks are still flowering and cannot reach the whole of the native resources of the mobile. We intend to evolve/move our platform to support state-of-the-art technologies such as the NFC, and these Frameworks are likely to pose a blocking.

We chose to develop the Mobile customer under Android technology in a first place; we chose this technology considering it is most dominant compared to other mobile technologies.

The mobile operating system Android in first position with 79% of market share is followed of iOs with 14,2% of market share (Figure 7).

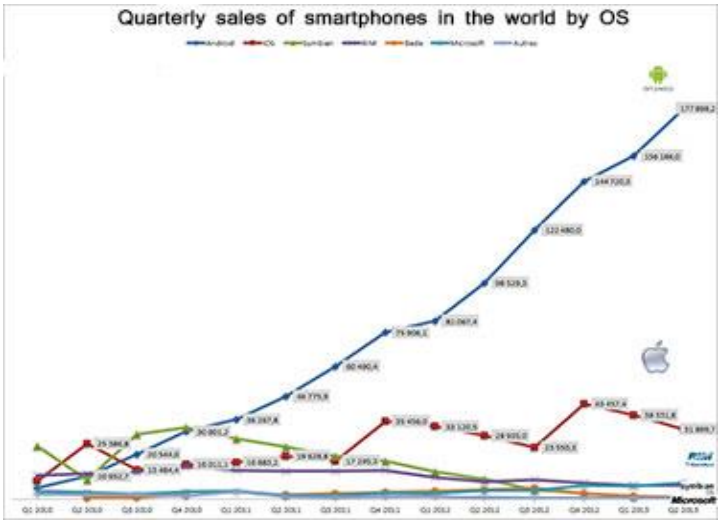

Fig. 7. Evolution of the market shares of the bones for smartphones (Android, iOS, Windows Mobile, RIM) # Gartner

1) The Web mobile services : The access to the Web services of the mediation system via the mobile is carried out using bookstore KSOAP2 [12], it provides a library of light and effective customer SOAP for the Android platform. It is Fork of the library kSOAP2 which is tested mainly on the Android platform, but should also function on other platforms using of the libraries Java [13].

B. The mediation system

For the development of the platform, we chose the J2EE technology in particular the JSP/Servlet, which is the standard of development of the applications of distributed companies, guaranteeing the robustness the evolution and safety [14], the richness of the bookstores and technologies and the weak blow of developments.

The application server used to implement the platform is the Tomcat server, which is a server of application supporting the JSP /Servlet [15]. Webservices are created by using Axis, the Apache solution, which is the Open Source container of Webservices more dominating [16].

1) The Web services SOAP : Although technology REST (REpresentational State Transfer) is more popular in the fields of the developments Web/mobile (Figure 8) considering its simplicity to implement, it was even adopted by the large firms of the Web world such as Amazon instead of SOAP, it is well-known that it is limited to the level safety.

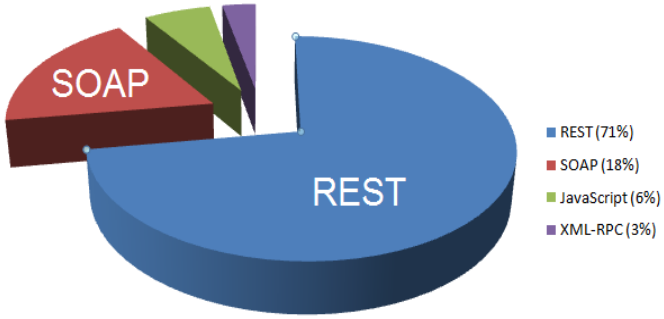

Fig. 8. Classification API web development. February 2012.

Technology REST is used mainly to make easy the access to the resources on the Web, while being based on protocol HTTP, via verbs which are defined by methods HTTP like DELETE, GET, POST and COULD, and it is from there that it holds are success, nevertheless although this technology was adopted by large firms of the Web such as Amazon [18], it still presents some limits. REST is a synchronous protocol and without state. When a customer subjects a request to the server, it does not have the means to know if its request were received automatically, but it is the server which must create a new task to inform the customer [19]. In our case, the platform is used especially for the operations of payment, therefore we need a robust and made safe technology, and this is why we chose an architecture SOAP.

2) Technology NFC : Near Field Communication, is a wireless technology for short-range use the mobile phone as a payment close [20].

In the short term we have used this technology to:

- Strong client authentication via an NFC card:

The platform offers customers the ability to use NFC as a method of physical security.

At the time of account creation, at the Security menu, the client begins by asking the setting of its new NFC card, the platform generates a key using HSM "Hardware Security Module" which will be sent to the customer's phone, the mobile application loads programming the Tag in the NFC card, the customer can choose the NFC card as the only means of authentication.

Therefore, the connection to the platform becomes easier because the client no longer need to enter their email address and password to log in, but just simply put his card on his NFC phone.

On the other hand at the time of payment services, the platform requires the client to validate his basket with NFC card.

In this way, we reduced the security risks for theft of telephone or mobile phone use by a third party.

- The transfer of money between customers:

The second use of NFC card money transfers between customers of the platform, or payment at the point of sale.

The money transfer is done via the mobile application, by entering the amount to be transferred, to validate the customer only has to ring closer its phone the recipient to complete the transaction. The mobile application retrieves the identifier of the recipient on this NFC card or Mobile phone (supporting NFC) and transmits to the platform a request for money transfer with the amount and beneficiary identifier.

VII. THE ASPECT SAFETY

To guarantee the security of our system, we propose to use PAD-DSS standard and the material potential of the smartphones in terms of safety:

A. PA-DSS standard

Currently, the financial institutions are conscious of the risks of safety, of the new standards were forced to reduce the risks of safety of the applications of payment in particular the standard PA-DSS, which is the program managed by the Council supervising before the program of Visa Inc. The goal of the PA-DSS is to help the suppliers of software and others to develop protected applications of payment which do not memorize data prohibited, such as the complete magnetic bands, the CSC number ("Card Security Code") or the data of PIN (“Personal Identification Number”), and to make sure that their applications of payment are in conformity with NCV DSS [21].

This standard has been implemented in our platform by:

1) Log: Avoid drawing confidential information in the logs to prevent any holdings of these data by an administrator.

2) The credit card information: stored on the platform are encrypted using RSA method, and they are hidden at the time of posting to the administrator.

3) OWASP implementation: At the platform level the possibility of the OWASP implementation library providing a source code open source to avoid the Ten Application Security Risks of the Most Critical Web. Ranked by various security agencies (DoD, PCI Security Standard)

B. Material

In addition, we will exploit the last tendencies of the mobile potential to make more safety and robust our solution, in particular, by using, the identification by digital fingerprint, the physical identification by NFC card, and the geolocation.

C. Prevent money laundering

To avoid bleaching and embezzlement, we propose to set up a data mining system to detect suspicious behavior based on data from the database "Transactional Log" by complying with rules such as:

- Do I know the customer?

- Is the transaction is consistent and compatible with the habits of the customer?

- This transaction is logical?

On the other hand the system checks the transaction amount, the position of the client and geolocation services purchased to control any possible fraud operation.

D. Two factor authentication:

The disadvantages of using NFC card for authentication, is that this key should be transported anywhere with the customer, if the customer risk for loss of the card not being able to access their account.

So for customer recognition, we have designed several authentication methods, taking into account available on the mobile phone technology.

The simplest method of authentication is the Email address and password, this mode presents security risks if a third party had access to this information, another layer of security that can be added to this mode is checking imei code of the phone or the phone number to see if it is indeed the owner of the account to make the payment.

NFC card: the platform provides a physical means which is the NFC card to authenticate the client, which in case of theft of the phone, the thief need this card to make these payments. setting the card passes through the customer's mobile phone during setup and the customer has the ability to generate a pin code on its NFC card in order to get his account for the loss of NFC card.

The fingerprint: We are currently testing a new API called Fingerprint_SDK, introduced by Samsung for its Galaxy mobile phone S5 enables developers to exploit the fingerprint chip in their projects. This API provides default parallel fingerprint the possibility for the user to enter a PIN if there are problems with the fingerprint authentication.

VIII. CONCLUSION AND PROSPECTS

This is a proposal for a mediation system based on the mobile phone, we noticed that the market of the smartphones

gains ground in the next future years and we want profited from his potential to offer a solution has low costs, while guaranteeing the standards of performances and safety required in this field. Currently we are in the final phase of the development of the platform, the model under development and limited only to the payment of bills, knowing that the use of the platform is able to support other services. On the other hand we have limited the use of NFC technology for authentication and transfer of money, we are studying the prospects of using this technology in the platform, to extend it to the automation purchase tickets by NFC or RFID (Radio Frequency IDentification) [22]. We also plan to test security with robots to test the behavior of the platform against attacks and transactional response time. These results will be published in another article soon.

REFERENCES

[1] International Telecommunication Union,May 2013,WTID 2013.

[2] Gartner,"Worldwide Mobile Device Sales to End Users by Vendor",May 2012.

[3] Infogile Technologies, "Mobile Banking – The Future", August 2007 .

[4] Gartner "Market Share Analysis: Mobile Phones, Worldwide, 2Q13.".

[5] Ravi Tandon , Swarup Mandal and Debashis Saha, M-Commerce-Issues and Challenges.

[6] FICO by Euromonitor International http://fico.com/landing/fraudeurope2013/,2013.

[7] IACSIT, "Mobile Commerce and Related Mobile Security Issues »,2011.

[8] Agilent Technologies, Agilent VISA User's Guide".

[9] BANK FOR INTERNATIONAL SETTLEMENTS, "Payment, clearing and settlement systems in the CPSS countries Volume 2" ,November 2012.

[10] PhoneGap website, http://phonegap.com/.

[11] JqueryMobile website, http://jquerymobile.com/.

[12] KSOAP Poject website,http://kobjects.org/ksoap2/index.html.

[13] KSOAP for android,https://code.google.com/p/ksoap2-android.

[14] John Roth, SAS Institute Inc., Cary, NC "Configuring J2EE Application Servers for Use with the SAS BI Platform".

[15] Apache Tomcat Website, http://tomcat.apache.org/tomcat-5.5-doc/index.html.

[16] Beytullah Yildiz, Telecommunications, 2006. AICT-ICIW '06. International Conference on Internet and Web Applications and Services/Advanced International Conference on, "Experiences in Deploying Services within the Axis Container".

[17] Jerry Gao, Krishnaveni Edunuru, Jacky Cai, and Simon Shim, IEEE International Workshop on Mobile Commerce and Services (WMCS'05),"P2P-Paid: A Peer-to-Peer Wireless Payment System".

[18] Tim O'Reilly, O'Reilly," REST vs. SOAP at Amazon".

[19] National Security Agency USA," Guidelines for Implementation of REST" ,2011.

[20] Tom Igoe, Don Coleman & Brian Jepson , O'Reilly,"Beginning NFC: Near-Field Communication with Arduino, Android, and PhoneGap" ,2014.

[21] Pci Security Standards Council, "Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) " , 2014.

[22] Mabel Vazquez-Briseno, Interactive Multimedia Edited by Ioannis Deliyannis, "Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World" , March 7, 2012.

[23] T. Kippenberger, Fasten your seatbelts, The Antidote 5 (1)(2000) 38–39.

[24] S. Kumar, J. Stokkeland, Evolution of GPS technology and its subsequent use in commercial markets, International Journal of Mobile Communications 1 (1/2) 2003) 180–193.

[25] H. Vogt, F.C. Gartner, H. Pagnia, Supporting fair exchange in mobile environments, Mobile Networks and Applications 8 (2) (2003) 127–136.

[26] E.W.T. Ngai, A. Gunasekaran , July 2005, "A review for mobile commerce research and applications", International Journal of Business Innovation and Research.

[27] Ashutosh Saxena, Manik Lal, Das Anurag Gupta, IEEE International Conference on Mobile Business (ICMB'05) "MMPS: A Versatile Mobile-to-Mobile Payment System".

[28] Rahul Gaikwad, Mr. Shubham Chaudhari, Ms. Dhanwanti Gaikwad, International Journal of Electrical and Electronics Engineering (IJEEE) 2011, "An Integrated Mobile Phone Payment System Based on 3G Network"