International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-4)

Research Article | **April 2014**

A Secure M-Payment Protocol for Mobile Devices

Prof. Vina Lomte, Swapnil Deshmukh, Subodh Jadhav, Vinod Munde
Padmabhooshan Vasantdada Patil Institute Of Technology,
Pune, India

Abstract:

Mobile devices, such as cell phones, and PDAs are becoming more popular each day. The large number of mobile users along with the ubiquitous nature of mobile devices has created a huge market for mobile commerce. But for that market to be realized users have to trust the security measures of m-commerce in general and m-payment in particular. In this paper a secure m-payment protocol for mobile devices has been proposed. The main objective in the proposed technique is to have the highest impact, and acceptance among average users. Hence, GSM the fastest growing network that accounts for 75% of the world's digital mobile market is selected as the network. For wider acceptance the simple and user friendly SMS text messaging protocol is selected as the transport channel. The proposed technique is independent of security measures and the systems inside banks and financial institutions. A pilot version of the protocol has been implemented. Simulation results, presented in this paper, indicate that the protocol achieves the expected level of security and can manage most security attacks, while remaining cost effective and easy to use for both the users, and the service providers

Keywords: m-payment, sms text message, SSMS protocol, mobile device.

I. INTRODUCTION

M-payment (mobile payment) is a point-of-sale payment made through a mobile device, such as a cellular telephone, a smartphone, or a personal digital assistant (PDA). Using m-payment, a person with a wireless device could pay for items in a store or settle a restaurant bill without interacting with any staff member. So, for example, if a restaurant patron wanted to pay quickly and leave the restaurant on time to get to an appointment, the bill could be paid directly from the table - without waiting for a server to bring the check. The patron would simply connect to the cash register with a wireless device, punch in the table number and bank personal identification number (PIN), and authorize payment. According to Orange Mobile Payment (a Danish company), the entire transaction should take no more than 10 seconds.

II. LITERATURE REVIEW

The prime actors in the mobile payment services market are mobile payment service providers and their customers. Various parties assuming these roles in the market include consumers, merchants, financial institutions and telecom operators. Additional parties, typically vendors of handsets, software, networks and other technologies may also be involved. The power and the interests of these parties impact how technologies and other resources are orchestrated into mobile payment services, and how these services are offered to and used by the market. Moreover, mobile payment services compete for the attention of customers and other parties against physical and electronic payment services. Mobile payment services are a natural choice to pay for mobile services. Yet, to succeed, mobile payment services may have to offer added value and be available for other relevant payment environments as well. In addition to the competitive forces within the mobile payments services markets, other factors are believed to impact these markets as well, for example, technology and standards, regulatory activities and legislation, established purchase and payment habits, or national economy infrastructures. If we regard a mobile payment services market as the unit of analysis (organization), these other factors become contingency factors, which influence the performance of the unit but are beyond the influence and control of that unit, as defined in the contingency theory. Contingency theory therefore is also well suited to classify mobile payments research and to capture the environmental factors which are characteristic to the mobile payment services markets.

III. PROPOSE SYSTEM

A. Purpose

The main objective in the proposed technique is to have the highest impact, and acceptance among average users. Hence, GSM the fastest growing network that accounts for 75% of the world's digital mobile market is selected as the network. For wider acceptance the simple and user friendly SMS text messaging protocol is selected as the transport channel.

The proposed technique will work in shopping malls where people will be able make payment simply via text message without compromising on security.

Text Message includes
<<RECI_ACC_NO>> <<AMOUNT>> <<PASSWORD>>

B. Architecture

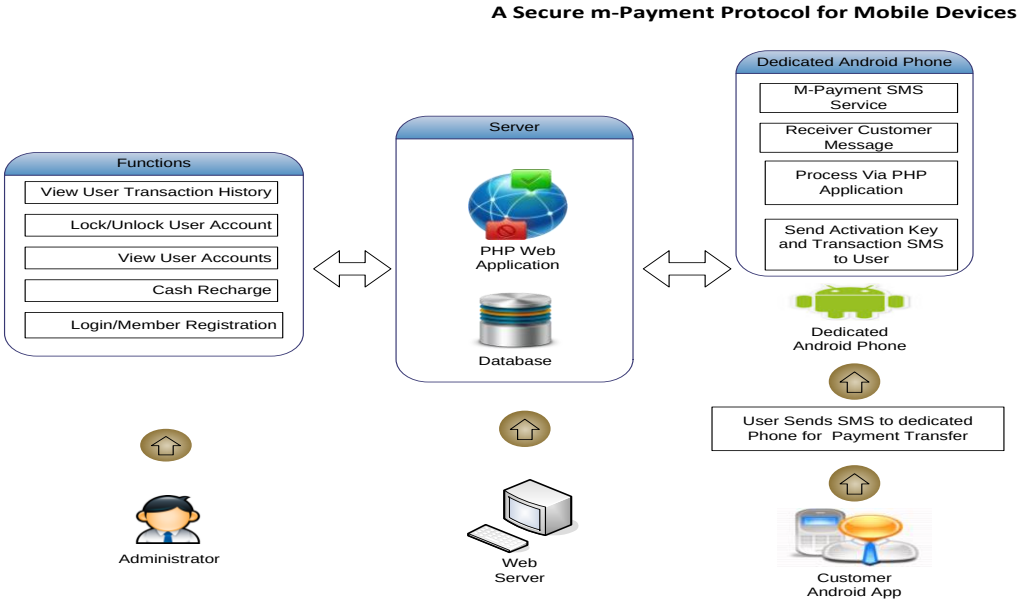


Fig. 1 Architecture of m-payment protocol

C. Mathematical Model

Problem statement: To build an application helps user to have secure authentication by using graphical session passwords.

1. *Problem description*

Let,

S is the system such that S= {U, L, L', SA, SA', SC, SC', T}

U is the set of system users U = {U_1, U_2, U_3…. U_n}

L is the set of logins which are successful L = {L_1, L_2, L_3….L_n}

L' is the set of logins which are not successful L = {L_1', L_2', L_3'….L_n'}

SA is the set of alphabetical sessions that user uses SA= {SA_1, SA_2, SA_3….SA_n}

SA' is the set of alphabetical sessions that user uses SA'= {SA_1', SA_2', SA_3'….SA_n'}

SC is the set of color sessions that user uses SC= {SC_1, SC_2, SC_3….SC_n}

SC' is the set of color sessions that user uses SC'= {SC_1', SC_2', SC_3'….SC_n'}

T is the set of tasks that the user does to login T = {T_1, T_2, T_3….T_n}

Set Theory **:**

Definition Module A :

$A_{i/p}$ = {Ai_1 , Ai_2, Ai_3…….Ai_N }

Where Ai_i consists of output set $B_{o/p}$ of module B.

$A_{o/p}$ = {Aj_1 , Aj_2, Aj_3…….Aj_N }

Where Aj_j contains set of variables which stores validated clients.

Definition Module B :

$B_{i/p}$ = {Bi_1, Bi_2 , Bi_3 …… Bi_N }

Where Bi_i is client and i = 1 to n having set of attributes as

{ I_1 : Accept Data , I_2 : Validate data , I_3 : Store Information ,

I_4 : Register admin }

$B_{o/p}$ = { Bj_1, Bj_2 , Bj_3 …… Bj_N }

Where Bj_j is client and j = 1 to n having set of attributes as

{ J_1 : Validated Client,J_2 : Registered Client , J_3 : Store Information,

J_4 : Approved access to client }

Definition Module C :

C set is a set having input directly from client side i.e from set $B_{i/p}$.

C_{legal} is a set defined as a set of all legal or approved clients and

$C_{illegal}$ is a set defined as a set of all illegal or rejected clients.

$C_{i/p}$ set of inputs to the module C defined as

$C_{i/p}$ = {C_1,C_2,C_3…….C_N}

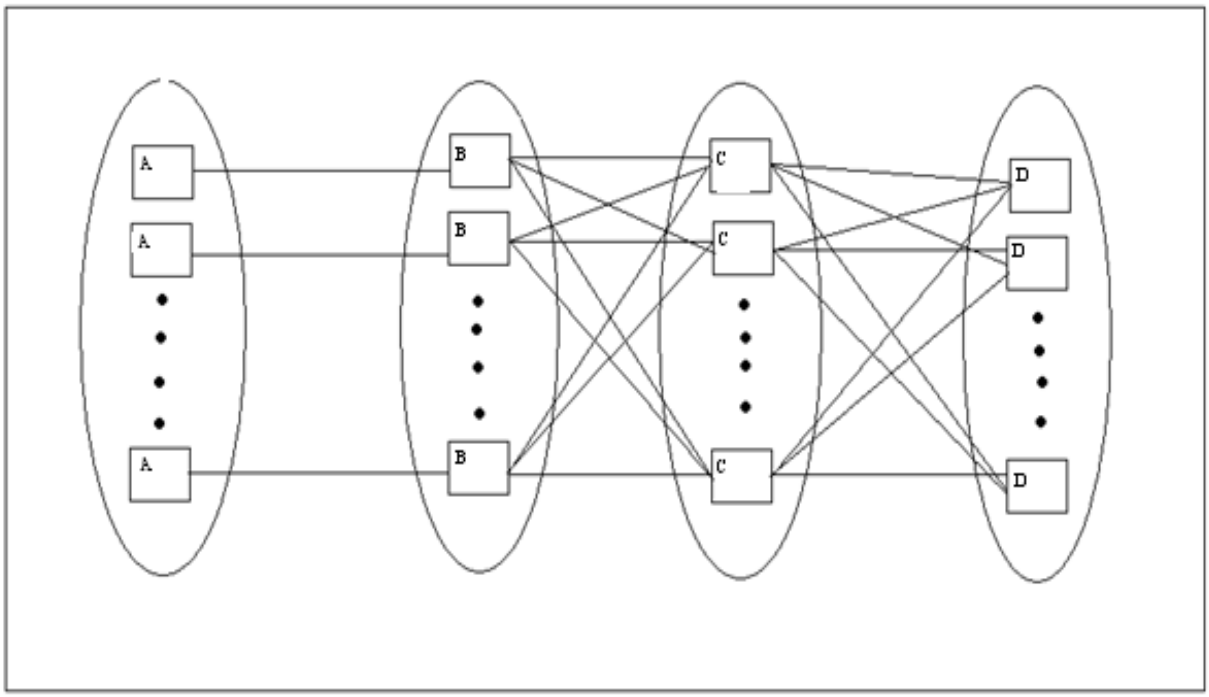
Where C_i is client and i = 1 to n having set of attributes as

{ I_1 : Unique Id , I_2 : Verified data proof }

C module is a module of authentication. So it validates data as per stored information. And takes they decision for approving admin access.

$C_{o/p}$ = { Cj_1, Cj_2 , Cj_3 ..... Cj_N }

Where Cj_i is client and j = 1 to n having i belongs to the $C_{legal.}$



Representation of proposed System as per basic rules of Set theory **:**

1. $B_{o/p} = B_{i/p}$ U B_{proc}
   Where B_{proc} is set of processes taking place in module B.
2. A = $_{def}$ { x | x ϵ B}
3. A intersection B = $_{def}$ { x | x ϵ $B_{i/p}$ AND $B_{i/p}$ AND $A_{i/p}$ }
4. $B_{o/p}$ ϵ A
5. $C_{i/p}$ subset A
6. $C_{o/p}$ subset A
7. A – B = $_{def}$ { x | x ϵ C_{legal} AND x Not belongs to $C_{illegal}$ }
8. $C_{o/p}$ subset B
9. B = $_{def}$ { x | x ϵ $C_{o/p}$}
10. B X C = $_{def}$ { (x,y) | x ϵ $C_{o/p}$ AND y ϵ C_{legal} }

D. Algorithm

Input: user id, password
Output: service successfully provides.
1) Get IMEI and cell id
2) If user already exist then
   User is ready to use application and is connect online
   Else
   Create new user and save the data in database
3) Check if user device is GPS or NON-GPS
   If user having GPS then
   Get his location on the basis of longitude
   Else
   Fetch his cell id from cell and send it to server
4) If user hits menu key
   Then provide services
   Else
   Go to step 1
5) Exit

IV. FEASIBILITY STUDY

Feasibility study is performed to determine the possibility or probability of either improving the existing system or developing a completely new system. Following are the feasibilities, which are considered for the development of the application:

- Operational Feasibility: It means to estimate whether it is required to the train the user to handle the system. In this case there is only training of interaction with user interface. Since the users are computer literate it would not to be difficult to adapt to new system.
- Technical Feasibility: Technical feasibility is to estimate whether it is possible to develop the proposed system with the available hardware and software and network resources. Since all proposed hardware, software and network requirements are easily available; the development of the application is feasible.

We can prove that our system is NP-Complete because in our system the most complex module is administrator module but it is implemented in non polynomial time. So our can be considered as NP-Complete.

To prove that the system is NP-Complete , we will use the AND/OR Graph decision problems:

- The AND/OR Graph decision problem states that while solving the complex problem, it broken down into series of sub-problems. These sub-problems can be further decomposed into sub-sub-problems. To obtain the solution to main problem the solution to any sub-tree can be sufficient. We can choose the better solution and discard other solutions.
- Similarly in our system decision is done by administrator to choose one team amongst the various teams in which they are expertise in according to the requirement . Then the team is decomposed of various team members, from this particular team we can get the project done.

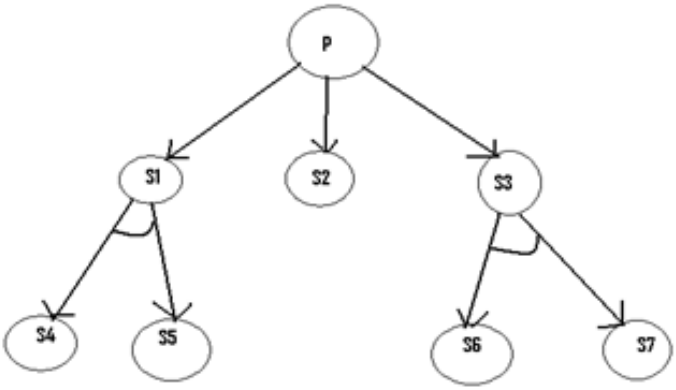


Fig. 2 AND OR Graph on Administrator Module

Here P is Administrator , S1,S2, and S3 are different teams from which P can selet any of the teams as solutions, Node S1 is AND node i.e. we can get the solutions from S4 and S5 where S4 and S5 are team members of the particular team. Thus the problem is solvable so our system is NP-Complete.

V. SYSTEM FEATURES

A. *Functional Requirements*

- User authentication using user id and password
- Face detection and training engine
- Face Recognition engine.
- Android Project
  It should implement and extend the messaging facility of android phone to send/receive SMS. All user payment messages are received on android phone and then processed.
- Web Based M-Wallet App
  It should provide a web based interface to all the application users. User should be able to recharge their account, view balance statement. Admin should be able to register users and check account history. Admin should be able to lock/unlock account in case of any problems.
- Client Application for M-Payment
  Client should be able to make payment using simple SMS.

B. *Non-functional Requirements*

- Secure access of confidential data (user's details). SSL can be used.
- 24 X 7 availability.
- Better component design to get better performance at peak time.

- Flexible service based architecture will be highly desirable for future extension
- Ease of Use- Few clicks, intuitive, flexibility, performance and installing/download.
- Security- Privacy, Confidentiality, Integrity, Authentication, Verification/Non-repudiation.
- Comprehensiveness- Transferability, Divisibility, Standardization.
- Expenses- Setup Fees, Transaction Fess, Subscription Fees.
- Technical Acceptability- Integration Effort, Interoperability, Scalability, Remote Access, Performance.

VI. FUTURE SCOPE

Security has been an issue of M-Commerce development right from the start of this effort. Current infrastructures considering the limitations and enhancements, offer a comfortable environment for secure mobile payment transactions.

Many challenges are involved in building an m-commerce solution, and just as many solutions available on the market. The comprehensive m-payment suite combines strategy and analysis with rapid, fully customized technical solution development and implementation, resulting in a high return on the investments. The above proposed models of mobile payments are easy to implement considering the available technology infrastructure. The models are simple, secure and scalable. The specific workflow implementation depends on user's disposition in motion. As a light motive, the enterprises with multichannel infrastructure have to harmonize the security level for m-payment and web-based security architectures for m-payment in order to protect their business and build future-proof architectures.

VII. CONCULSION

In this paper we proposed a secure payment protocol, considering the restrictions of mobile networks in developing countries. The proposed protocol not only satisfies the convenience and ease of use that is generally required for mobile users in small payments, it also provides the transaction security level and non repudiation property that is necessary for macro payments. Although the proposed technique has been optimized for the current GSM network, but its modular design enables it to accept future improvements of the mobile network technology and infrastructure, such as EMS and MMS, with minimum change in the protocol structure.

ACKNOWLEDGMENTS

We are greatly indebted to our college Padmabhooshan Vasantdada Patil Institute Of Technology that has provided a healthy environment to drive us to do this project and thankful to our management for their guidance

REFERENCES

[1] . Juniper Research, August 2004, www.Juniperresearch.com
[2] “Mobile commerce report”, *Durlacher Research Ltd.* 2003
[3] “Enabling Secure, Interoperable and User friendly mobile payments”, *Mobile Payment Forum white paper*, December, 2002, MobilePaymentForum.com
[4] "Mobile payment report", Published by: Eurotechnology Japan, K.K, 2005/04
[5] Mobile Electronic Transactions. (2001). “MeT Account-Based Payment,” http://www.mobiletransaction.org/pdf/ MeTAccount-Based-Payment-20010221.pdf
[6] Mobay Forum, Mobile financial services, (2001). "The preferred payment architecture technical documents" www.mobeyforum.org/public/ material/PPATechnical.pdf
[7] A. Basaure “Preliminary research on existing and planned mobile data service solutions and value systems in leading markets”, *Helsinki University of Technology HUT*, 2004
[8] Tom O'Leary, " SMS Messaging: How is Your Text Life?" January 03, 2006, http://www.infacta.com
[9] WAP Forum, “WAP Architecture: Wireless Application Protocol Architecture Specification,” 2001, http://www.wapforum.org
[10] N.R. Potlapally, S. Ravi, A. Raghunathan,” Analyzing the energy consumption of security protocols”, *Princeton University, ACM Digital Library*, 2003.
[11] C. H. Gebotys," Low Energy Security Optimization in Embedded Cryptographic Systems",*University of Waterloo, ACM Digital Library*, 2004
[12] V. Gupta, S. Gupta, S. Chang, and D. Stebila, “Performance analysis of elliptic curve cryptography for SSL,” in *Proc. ACM workshop. Wireless Security*, pp. 87–94, Sept. 2002.
[13] Mobile Payment Forum, white paper, “Risks and threats analysis and security best practices”, 2003.