Building Robust m-Commerce Payment System on Offline Wireless Network

Chitra Kiran N.
Asst. Prof: Dept of Electronics & Communication Engg.
Sai Vidya Institute of Technology
Bangalore, India
E-Mail: chitrakiran2002@yahoo.co.in

Dr. G. Narendra Kumar
Prof. Dept. of Electronics & Communication Engg.
UVCE
Bangalore, India
E-Mail: gnarenk@yahoo.com

***Abstract*— Mobile commerce is one of the upcoming research area with focus on mobile payment systems. Unfortunately, the current payment systems is directly dependent on fixed infrastructure of network (cellular network), which fails to facilitate optimal level of security for the payment system. The proposed system highlights a novel approach for building a secure, scalable, and flexible e-payment systems in the distributed scenario of wireless adhoc network in offline mode of communication for enhanced security on transaction and payment process. The proposed system uses Simple Public Key Infrastructure for providing the security in payment processes. The performance analysis of the proposed model shows that the system is highly robust and secure ensuring anonymity, privacy, non-repudiation offline payment system over wireless adhoc network**

Keywords-e-payment, wireless adhoc network, mobile commerce

I. INTRODUCTION

Mobile payment is the financial transactions for some services or good between the trading parties through mobile terminals [1]. Majority of the payment system currently in use consider online communication with the network and is much infrastructure dependent, which is very different scene compared to wireless mobile adhoc network. The use of digital coin is also in abundant but it has been seen that digital coin usage generates security issues as well as privacy issues. Currently, researchers has focused on the e-payment system such that electronic cash [2-7], electronic check [8-9], electronic traveler's check [10-11] and so on which has plenty of computational resources such that exponential operation thereby causing the big burden for the system. The proposed system is based on the secure and reliable transaction being carried out in an offline connection in wireless adhoc network. The proposed system is standardized with respect to communication system where it facilitates ease in deployment for clients. Although there are some effective research being done in the area of payment system, but there is a huge research gap in this area with respect to wireless mobile adhoc network.

The proposed model will amalgamate into the hierarchical transaction system which facilitates the clients to conduct transaction both in online as well as in offline connection with reliable security measures. The proposed architecture is designed for security features using simple public key infrastructure which integrates elasticity to the use of e-cheque in offline mode using digital coins. The IETF Simple Public Key Infrastructure Working Group is tasked with producing a certificate structure and operating procedure to meet the needs of the Internet community for trust management in as easy, simple and extensible a way as possible. The SPKI is intended to provide mechanisms to support security in a wide range of Internet applications, including IPSEC protocols, encrypted electronic mail and WWW documents, payment protocols, and any other application which will require the use of public key certificates and the ability to access them. It is intended that the Simple Public Key Infrastructure will support a range of trust models. The certificate authorization of Simple Public Key Infrastructure which combines authorization to the public key is mechanized in the proposed system in order to combine authorization for mobile commercial payment to a user's key. The best feature of this model is its ability to delegate the authorization to other clients using a chain of delegates. The payment mechanism of the proposed system is shown in Fig 1.

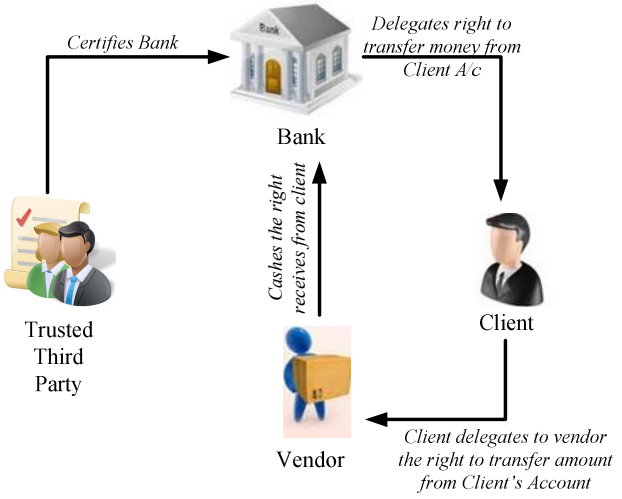

Fig.1. Payment mechanism in proposed system

The bank is certified by the trusted third party in the initial stage, which is done using authentication certificate for bank. In the consecutive phase, bank transmits an authorization

certificate to Clients, which consist of authorization to its client C to transfer amount from client's account to the bank. The delegation flag is configured by bank which permits client to delegate this permission. Both the verification certificate along with recently designed verification certificate is transferred to client by bank. The bank identity as well as the validity of the authorization certificate of client is evaluated by client in order to check if TTP has signed the authorization certificate of bank and bank has certified that for the client. Then, client generates a new permission certificate for the vendor for transferring his rights to vendor to transfer amount from client's account. The security of the proposed system is maintained by this architecture where by implementing simple public key infrastructure by confining the rights of withdrawal. The entire cumulative certificate chain is transferred by client to vendor who analyzes its authenticity. The final stage of verification is done by bank when vendor transfers the chain to bank. The validity of the certificate is evaluated by bank to check the genuine source of the certificate (bank). After successful validation, the vendor is privileged to withdraw amount from client's account. The authorization certificate which is frequently used consists of flag shows the validity of binding authorization and its respective delegation which is one of the prime factor of security. The proposed system assumes all the independent modules (TTP, bank, client, vendor etc) as certificate authority which is very suitable for any distributed architecture of wireless mobile adhoc network. The system reserves the chain used as it consists of confidential information related to the payment system as well as means to recognize cyber illegal users.

II. ARCHITECTURE DESIGN

The main motive for the highlighted methodology is to build an effective and secure e-commerce system in wireless mobile adhoc network. The proposed system highlights a very flexible architecture for secure transaction in wireless mobile adhoc network.

The architecture as shown in Fig.2 is basically classified into two main blocks e.g. first is *PaymentEngine* and second is *SecurityEngine*. The first block i.e. *PaymentEngine* basically has repository of certificates for the proposed payment schemes e.g. authorization certificates, authentication certificates, account permissions etc. The first block provides an interface for notification in direct communication with updating of repository. The maintenance user interface communicates with user. The user can be considered as innermost payment service on the machine of user. The first block i.e. *PaymentEngine* deploys the 2nd block i.e. *SecurityEngine* for signing and validating chains of certificate. The security design is accomplished by using Simple Public Key Infrastructure using cryptographic framework in java which facilitates services for signing and creating chains of certificates.

According to this architecture, bank request for a digital certificate by TTP previous to any transactions to be permitted which is quite independent from any renewal. After this bank is prepared to transfer account permission to the clients assuming all the communication is done from mobile interface in wireless adhoc network.

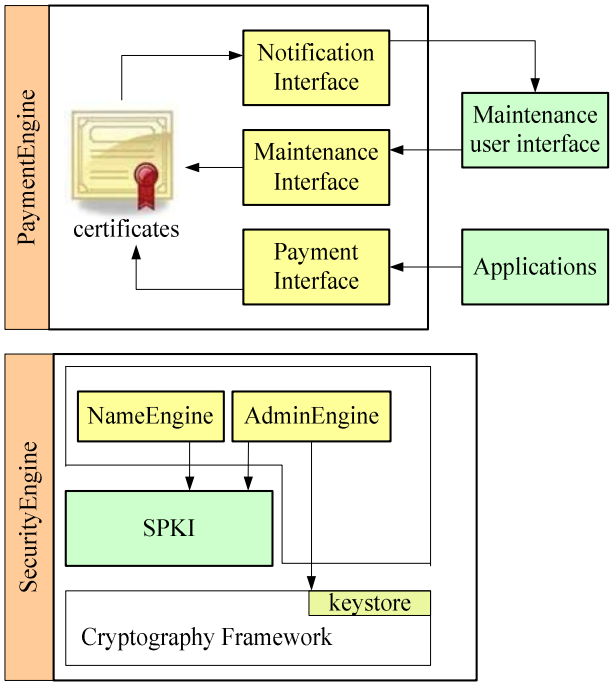

Fig. 2. Architecture of the proposed system

The bank again receives its public key from client and client checks his status of permission for accessing his account assuming client has an account with bank. Exactly after the previous step is accomplished, bank generates a new permission certificate and sent it to client. Now the client is prepared to communicate with vendor for payment scheme.

In the second phase of the transaction, when client communicates with vendor related to specific business transaction, the vendor sends a signed e-bill which includes list of TTP as there are many global TTP which user might not rely all. Client only evaluates if bank is authorized by at least one of the TTP which is conventional for vendor for secure future transaction. The communication / transaction between client and bank will fail if both the party does not have certain common TTP. The transaction duration is made secured by estimating validity duration for payment. The client then generates a deposit certificate and transfers the entire chain of certificate to vendor. The vendor accepts and evaluates the entire validity of chain. It is to be noted that for security reason, the certificate is valid for only one transaction for vendor.

One of important issue with communication on offline in wireless adhoc network is that account permission for client is feasible for being invalidated without vendor module knowing about it. In order to solve this issue, the proposed system highlights account permission with very short validity duration where bank should renew certificates frequently. Therefore if the certificate has been invalidated or rejected by the bank, than it will be subjected for acceptance offline for a very shorter duration. Therefore the proposed system with short term certificates has better security in the wireless mobile adhoc network.

III. Implementation and Analysis

The proposed system is implemented on 32-bit Windows OS with Dual Core Processor of 1.80 GHz. The coding is carried out in Java platform. The use of robust encryption along with digital signatures assures that proposed schema is not possible to illicitly decipher without specific private keys. The payment permission certificate is created only when there is a payment request and it will embed signature of both client and vendor. This is also used for identifying the dual deployment of client's payment permission certificate. The indisputability is involuntarily accomplished as all the payments are using digital signatures. The application also ensures non-traceability as flow of the transaction from one to another module can be reconstructed as the chain of certificate consists of public key of each chain. Therefore, no third person can identify the transaction information (other than bank). The propose system therefore facilities higher dimension of privacy and security. As the centralized service consisting of revocation list will not be accessible so invalidated certificates cannot be easily cancelled in office mode. This issue is solved by using short validity duration which needs to be renewed. Therefore the entire banking application can be integrated with the mobile application very secure in wireless mobile adhoc network in offline mode. Therefore the proposed system assures pseudonymity and restricts dual payments in one session. The proposed system offers concrete usability and high dimension of creating a flexible and extremely secure system for offline e-commerce in wireless mobile adhoc network. There is no requirement of creating a new technology or abstraction from scratch for any clients to use this application. Clients has higher flexibility to make custom-build identity, delegate payment permission etc, which will assist in creating much organized e-payment system in wireless network. Moreover as the Simple Public Key Infrastructure has no dependency on operating system, so it will be highly feasible to deploy the application on any trusted handheld device like smart phone or mobile handset with OS and browser. The proposed system his highly at par with the ubiquitous application of banking system as the application do not consider a constant network infrastructure as it is designed on wireless mobile adhoc network. Therefore, impulsive service and usage is guaranteed at any instance.

IV. Conclusions

The proposed system highlights a secure application for e-payment system in offline using wireless mobile adhoc network. The security of the application is governed by Simple Public Key Infrastructure. The formation of chains of certificate allows a distribution of the payment system by delegates. The designed model prevents dual expenditure in offline communication. The proposed system shows a flexible and robust solution for serviceability, security, and effectiveness in e-payment systems over wireless mobile adhoc network. The future enhancement work could be considered on design of security system based on specific attack on mobile adhoc network like DDoS or Wormhole attack, which is very common issue on pure mobile network deployment in larger scale of deployment.

References

[1] Haifeng Wu, Xuan Li, Weihui Dai, Weidong Zhao, "Mobile Payment Framework Based on 3G Network, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS '10) Guangzhou, P. R. China, 29-31, pp. 172-175, July 2010,

[2] C. Ellison, "SPKI Requirements", Network Working Group, Request for Comments: 2692, September 1999

[3] D. Chaum, "Blind signature for untraceable payments", In: Proceedings of advances in Cryptology, Springer-Verlag, New York, pp.199-203, 1983.

[4] W. S. Juang and H. T. Liaw, "A practical anonymous multi-authority e-cash scheme", Applied Mathematics and Computation, Vol. 147, No. 3, pp. 699-711, 2004.

[5] Y. Y. Chen, J. K. Jan, and C. L. Chen, "A novel proxy deposit protocol for e-cash systems", Applied Mathematics and Computation, Vol. 163, No. 2, pp. 869-877, 2005.

[6] C. L. Chen and M. H. Liu, "A traceable E-cash transfer system against blackmail via subliminal channel", Electronic Commerce Research and Applications, Vol. 8, No. 6, pp. 327-333, 2009.

[7] C. C. Chang and Y. P. Lai, "A flexible Date-attachment Scheme on E-cash", Computers & Security, Vol. 22, No. 2, pp.160-166, 2003.

[8] C. Ellison, "SPKI Requirements", Network Working Group, Request for Comments: 2692, September 1999

[9] D. Chaum, "Blind signature for untraceable payments", In: Proceedings of advances in Cryptology, Springer-Verlag, New York, pp.199-203, 1983

[10] J. E. Hsien, C. C. Hsueh, and C. Y. Chen, "An electronic traveler's check system", Conference on Theory and Practice for Electronic Commerce, pp. 164–169, 2001.

[11] H. T. Liaw, J. F. Lin, and W. C. Wu, "A new electronic traveler's check scheme based on one-way hash function", Electronic Commerce Research and Applications, Vol. 6, No. 4, pp. 499-508, 2007.