Chapter VI

Conclusion

An Architecture for Secure Mobile Payment System using Public Key Infrastructure
Chapter VI

CONCLUSION

Mobile Payment Systems and solutions focus now on authentication and integrity of data, but security service of non-repudiation needs more attention. Adoption of symmetric key, public key cryptography and Diffie-Hellman algorithm though useful and have advantages, yet there also are several limitations and problems. In view of the above aspects, this thesis proposes architecture for secure mobile payment system using Public Key Infrastructure through mobile devices.

The key features of the proposed architecture are the following:

- Design for payments in academic institutions by students to the institution’s authorized bank.
- Assured confidentiality, message integrity and non-repudiation by the use of strong encryption and decryption algorithms.
- Multi-factor authentication scheme
- End-to-end security
- Use of secret key for data transmission in the security algorithm
- Embedding encrypted public key on X.509 digital certificates

The noteworthy advantages are reduction of transactional cost and overhead time, applicability to all academic institutions and an ease to process payment.
Investigation by an establishment of a test bed at various levels has verified the performance of the proposed algorithm. The client side functional components are deployed at Sony Ericsson K750i - Java enabled mobile phone. The server functionalities are distributed to the Institution Server (IS), Mobile Payment Consortia System (MPCS) server, and simulated Certificate Authority (CA) server.

The experimental study has revealed that time spent on encryption of the UName and PWD by secret key is less than the use of RSA at client mobile device. The public key algorithm thus provides low response time and less performance at mobile phone compared with symmetric. However, it achieves high level security in terms of confidentiality and non-repudiation over symmetric algorithms.

The analysis of computational cost in MPCS security protocol as applied to the existing security protocol ensures high level security with reduction in the number of encryption operations. The proposed protocol proves its potential use in commerce and trade operations. Regarding the performance of the proposed system in terms of response times and system throughput in MPCS payment system, the proposed model exhibits a very scalable behavior.

Therefore, the proposed architecture in this thesis is a secure mobile payment system using Public Key Infrastructure. It overcomes the limitations encountered in the mobile payment systems proposed earlier.
FUTURE DIRECTIONS
This thesis suggests the following as directions for future research:

- The present research work is adopted for Consumer-to-Business (C2B) model. However, it is essential to investigate the deployment of proposed architecture into other payment models such as Consumer-to-Consumer (C2C) and Business-to-Business (B2B) with adequate level of security.

- It is necessary to study the new payment technology, such as Near Field Communication (NFC) for MPCS system, so that the mobile phone can be used like a contactless card, which will make the process more effective to the mobile users during payments.

- Since there is ever increasing percentage of mobile users, mobile payments have become more indispensable. As the technology changes the adaptability of mobile devices, network services and service providers are major bottlenecks for the common man. Since mobile network providers frequently change their scenario and operation, it is vital to design an integrated secure architecture for mobile payment system which can be adaptable by any network, any device and any payment etc.

- Finally, the scope for future research scope is on service-oriented architecture for secure mobile payment transactions which has to be initiated at the earliest in mobile devices. In spite of many contributions to
this effect offered by different researchers for mobile payments using web services, it is essential to combine the Web Services Policy (WS-Policy) framework and Web Ontology Language (OWL) to enhance the web service security.