An Integrated Approach for SMS Based Secure Mobile Banking in India

Neetesh Saxena, Narendra S. Chaudhari

Department of CSE, Indian Institute of Technology Indore, India

Introduction: M-banking can be executed using various channels like SMS, USSD, GPRS, WAP and phone based Application. Most of the people (70% of the population) living in rural areas of India don't have java enabled cell phones and Internet facility is also very limited through which WAP/GPRS based applications work. Nowadays, SMS is very popular and frequently used worldwide, however traditional SMS service does not provide any security to the transmitted message information. SMS based m-banking can be extended as a secure channel for users by enhancing the security of SMS. This concept of providing a secure channel can be implemented on a separate SIM. In India, most of the banks provide information retrieval services only and they don't permit to do transaction using SMS banking. Only banks can provide the facility of m-banking in India while in some other countries like Kenya and Philippines non-bank organizations can also provide such facilities. Apart from this, some banks provide change password through SMS which is a threat as SMS is not encrypted while transmitted to bank server.

Problem Statement: The main objective is to provide a secure mobile banking using SMS for the people who are living in the rural part of India and don't have java support cellular phones and Internet facility. Presently, SMS is not secure and is in clear text without any ciphering mode while transmitting. SMS and its banking environment must be prevented from various existing threats and attacks. Secure channel for banking is maintained by providing the security services authentication, confidentiality, integrity, non-repudiation.

Solving Approach: This new SIM is proposed to be issued by a government authorized body of the Telecommunication Department of India and store a shared key for each bank at the time of SIM manufacturing and in the database of respective banking server similar to the existing procedure. To manage the storage of SIM, we can limit a user to access 3 to 5 m-banking services of different banks at a time. This government authorized body integrates various service providers and different banks through a single and unique m-banking SIM. When a mobile user selects an option to choose a bank, a strong mutual authentication process takes place which involves session keys generated by the keys stored onto the SIM and in the database of bank servers. Since as per the Reserve Bank of India (RBI) guidelines only banks can provide such facility, thus it's a limitation where a particular bank can launch its m-banking SIM and users are limited to use the facility of that particular bank only. As per the proposed guidelines, users can choose their preferred service providers to do SMS based mobile banking of different banks. However, in order to ensure a secure channel for communication using a separated SIM, the current guidelines must be reviewed. Thus, an integration of service providers and different banks must be encouraged.

In this approach, first a mutual authentication takes place followed by a secure transmission of SMS to the banking server. SMS is encrypted using the symmetric cryptographic algorithm (like DES, Triple DES, AES, Blowfish, Twofish, CAST6, RC2 and RC6). The shared key is generated from the key stored onto the SIM as well as in bank's database. SMS contents along with user identity and timestamp are encrypted by the sender and are decrypted at banking server. This encryption prevents the SMS information from man-in-the-middle attack and timestamp prevents from the replay attack. To maintain the integrity of SMS, an authentication function (like MD5, SHA1, etc.) is implemented which prevents the SMS from SMS tampering and message disclosure. To prevent the system from repudiation attack, a digital signature algorithm (like RSA, DSA, ECDSA etc.) is implemented. SIM along with handset must be registered with bank database to prevent DoS and SMS spoof attacks. We have developed and implemented a new symmetric algorithm named MAES (modifies AES) which takes minimum time for ciphering as compared to the above mentioned algorithms. Apart from this, ECDSA is better for signature generation and verification. It takes less time and has strong structure that also reduces key size as compared to DSA. SHA-1 is used as message digest to maintain the integrity of message content.

Results: The platform used here is J2ME Wireless Toolkit for user interface, MySQL database and Tomcat as server. The results have been implemented with the JDK1.7 and J2ME wireless messaging API. Figure 1 and Figure 2 show the encryption and decryption time for symmetric algorithms. Out of these results MAES is best for ciphering where key with 256 bits is preferred over the 128 bits due to its strong cryptanalysis along with 256 bits block size. Figure 3 and Figure 4 present the implementation results of digital signature algorithms DSA and ECDSA, out of which ECDSA is optimum and consumes less time for signature generation and verification as compared to the DSA.

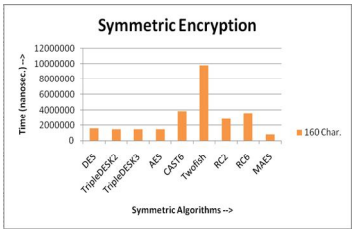

Fig. 1. Symmetric Encryption

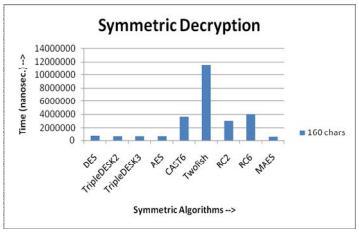

Fig. 2. Symmetric Decryption

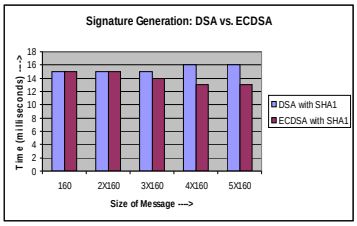

Fig. 3. Signature Generation

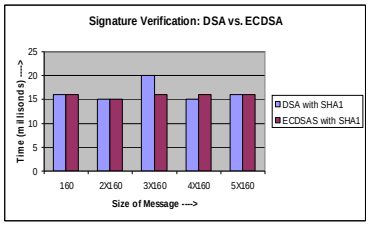

Fig. 4. Signature Verification

Future Work: **(**1) Confidence interval for the MAES algorithm for ciphering; (2) Storage space for each key and algorithm: used physical, virtual and swap memory size; (3) Energy & Time Efficiency: CPU time, Encryption/Decryption time, Key generation time; (4) Implement a variant of ECDSA algorithm which is more secure than the ECDSA (previous published work in ICMSAO-2013).