View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by International Journal of Science Engineering and Advance Technology (IJSEAT)

International Journal of Science Engineering and Advance Technology, IJSEAT, Vol. 4, Issue 4

ISSN 2321-6905
APRIL-2016

International Journal of Science Engineering and Advance Technology

A Secure Protocol for M-commerce Secure SMS Mobile Payment

Sai Dharma Reddy Gudimetla[1], BuddharajuShanmukh Varma[2], SaiRaghukanth Reddy Gudimetla[3]

[1]isecure payments (Android Developer),Gachibowli,Hyderabad, TG, India

[2,3]Gayatri Vidya Parishad College of Engineering, Visakhapatnam, AP, India

Abstract –

The worldwide utilization of the Internet has profoundly supplied the development of e-commerce. Technological advancement in mobile phones (e.g. Mobile phones) has likewise added to doing e-commerce by means of mobile phones (m-business). Mcommerce includes the utilization of mobile phones, for example, mobile phones in doing electronic exchanges. Applications in this area range from ordinary data utilization to high security money related electronic exchanges. Much the same as e-commerce, the security of m-business applications is basic, particularly when it includes applications that arrangement with client touchy information, In the usage, the purchaser utilizes the program to shop online of course, at the checkout he is sent to the versatile application gave and secured by the bank. The gatherings imparts through three distinctive channels (VPN burrowing, SMS informing and HTTPS) to improve the security. This convention guarantees that the purchaser basic data is never ignored the web to have the capacity to buy and in the meantime the scanning knowledge has little interference. Additionally it presents minimal overhead on the vendor and the banks to have the capacity to give such administration. To ensure the convention acts as expected, an android application was made that speaks with web servers speaking to the purchaser bank, the shipper site and vendor bank. All interchanges between the application and the purchaser bank were through VPN and SMS.

Keywords—SMS, SMS gateway,Banking and Mobile Services, Authentication, Mobile banking,Security.

I. Introduction

Three billion individuals are relied upon to possess mobile phones in the globe by 2012. There are presently 225 million mobile phones in India and 100 million are included each year. In a couple of years more than 500 million individuals are required to have mobile phones in India. Versatile commerce is a characteristic successor to electronic business. The ability to pay electronically combined with a site is the motor behind electronic commerce. Electronic commerce has been encouraged via Automatic Teller Machines (ATMs) and shared managing an account systems, charge and MasterCard frameworks, electronic cash and put away esteem applications and electronic bill presentment and payment frameworks. Versatile payments are a characteristic development e - payment conspires that will l encourage mobile business. A versatile payment or m-payment might be characterized, for our motivations, as any payment. Where a mobile phone is utilized to start, approve and affirm a commerce of money related quality consequently for products and administrations. Mobile phones may incorporate mobile phones, PDAs, remote tablets and whatever other gadget that interface with versatile telecom system and make it workable for payments to be made. The acknowledgment of mobile payments will make conceivable new and unexpected methods for comfort and business. Unsuspected Technological developments are conceivable are conceivable. A few versatile payment organizations and activities in EU have fizzled and numerous have been ended. In Europe and North America with couple of special cases, for example, Austria, Spain and Scandinavian nations the advancement of mobile payments has not been effective. Nonetheless, versatile payment administrations in Asia have been genuinely fruitful particularly in South Korea, Japan and other Asian nations (e.g., Mobile Suica, Edy, Moneta, Octopus,

and G Cash). NTT DoCoMo has 20 million endorsers and 1.5 million of them have actuated charge card usefulness in Japan. There are 100,000 peruses introduced in Japan. The fundamental distinction between fruitful usage of mobilepayment administrations in the Asia Pacific district and disappointment in Europe and North America is essentially credited to the 'payment society' of the purchasers that are nation particular. In this paper we exhibit an outline of the versatile innovation scene and location the attendant issues that emerge with the presentation of mobilepayment administrations. Versatile Commerce: Mobile Commerce is any exchange, including the exchange of proprietorship or rights to utilize products and administrations, which is started and/or finished by utilizing mobile access to PC interceded systems with the assistance of an electronic gadget.

Mobile Banking: Mobile saving money (M-Banking, SMS Banking) is a term utilized for performing equalization checks, account exchanges, payments and so forth by means of a mobile phone, for example, a mobile phone.

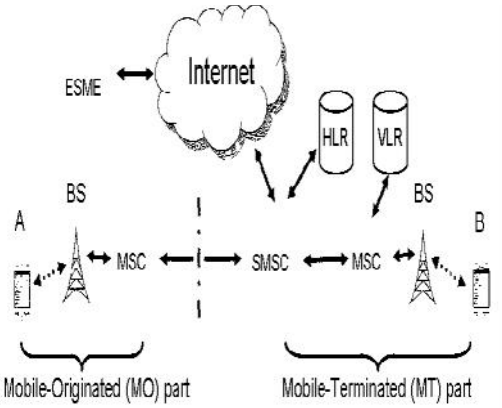
M-payment (mobilepayment): It is a state of-offer payment made through a mobile phone, for example, a PDA, Smartphone or individual advanced colleague (PDA). Payment utilizing a M-business gadget is typically called M-payment. [1]

II. RELATED WORK

As of not long ago, particular creators have proposed different procedures to offer security to the designated messages. An execution of open key cryptosystem for SMS in mobile phone system has been exhibited in java based open key foundation for SMS informing. A safe SMS is considered to give versatile commerce administrations exhibited in paper a high security structure for SMS and depends on open key cryptography [2]. A creator outline an application for secure extensible and proficient SMS transmission .This application is permit trading the message between two pears by utilizing open key cryptography [3]. Next application plan by the new creator called the SSMS. This new application outline for accomplishes the preferred security over the past one. This application is utilized for payment framework. For create the key in this application utilized the elliptic bend cryptography. This application gives the low data transfer capacity and practical arrangement [4]. Another application is additionally in view of the payment framework. This application depends on the high security establishment. This application creates the mutual key for every period and exchange the protected data between two companions [5]. Next application is configuration for the general human services. This application depends on the java open key cryptography. This application put away all the therapeutic information of every individual and secure message exchange starting with one mobile phone then onto the next [6]

III. SMS NETWORK ARCHITECTURE

SMS messages are transmitted over the Common Channel Signaling System 7 (SS7). SS7 is a worldwide standard that characterizes the methods and conventions for trading data among system components of wire line and remote phone bearers. These system components utilize the SS7 standard to commerce control data for call setup, directing, versatility administration, and so forth. Figure 1 demonstrates the common system engineering for SMS correspondence. Adroitly, the system engineering comprises of two portions that are integral to the SMS model of operation: the Mobile Originating (MO) part, which incorporates the versatile handset of the sender, a base station that gives the radio base to remote correspondences, and the starting Mobile Switching Center (MSC) that courses and switches all movement into and out of the phone framework in the interest of the sender. The other fragment, the Mobile Terminating (MT) part, incorporates a base station and the ending MSC for the collector, and also a brought together store-and-forward server known as SMS Center (SMSC). The SMSC is in charge of tolerating and putting away messages, recovering record status, and sending messages to the proposed beneficiaries.



IV. SMS SECURITY THREATS

Message Disclosure: In the SMS service message is transmitted as an unencrypted text. Message could be intercepted during transmission. SMS is first stored as an unencrypted text in the SMSC and then delivered to the destination receiver. This message could be viewed by the users in the SMSC.AES encryption approach secure the transmitted SMS from Message Disclosure attack.

Replay Attack: The attacker can misuse the already transmitted message between the user and network. The exclusive timestamp values can secure the message from the Replay Attack.

Man-in-the-middle Attack: When the user does not authenticate network then the attacker can use a different BTS with the same mobile network Id and then man-inthe-middle attack is perform. This attack can be prevented by the AES algorithm.

Denial of Service: Denial of Service attack is performing when sending repeatedly messages to the destination mobile phone.

SMS Viruses: There have been no reports of viruses with message when the message is transfer from one mobile device to another but mobile devices are getting more powerful and programmable. The SMS viruses being spread through the message.

V. OVERVIEW OF SMS SECURITY ALGORITHM

A. Data Encryption Standard Algorithm (DES)

Data Encryption Standard (DES) is most widely used encryption technique which is developed in 1997. It is the most important encryption scheme used to encrypt and decrypt the data.DES algorithm does not provide the strong security, because the many attacks is bombarded on the DES. The Data Encryption Standard consists of the larger key than the other algorithm and the data are encrypted in block [7].

The Data encryption standard provides an authentication courtesy to all the users. In DES algorithm consist of the keys to provide integrity and the authentication. The DES algorithm involves the personal identity verification code to verify the identity of the users. Author implemented an application which is used to secure the data which are transfer from the one user to another user [8]. Author develops an application to delegates the encrypted form of payment from one mobile to another mobile using the symmetric and asymmetric key cryptography. In the symmetric cryptography use the same key on sending and receiving end and in the asymmetric key cryptography use the different key on both ends [9].

The Data encryption standard consists of one more type i.e. Triple DES.The 3DES is the session key which is used for the encryption. The 3DES session key is used to encrypt the data when SMS is transfer between customer obile and the bank mobile. Many attacks are bombarded on the triple DES [10].

B. Advanced Encryption Standard Algorithm (AES)

Advanced Encryption Standard is based on the symmetric encryption technique. Advanced Encryption Standard provides a better security than the triple DES and the strength of the security is much better than the other. The key size of the AES is small as compared to the other scheme.AES consist of the byte substitution and the shift rows and these form the round transformation. Many attacks are bombarded on the algorithm and they can break the algorithm [1].

Author develops an SMS security application to provide the authentication and the integrity to the content of message. Advanced Encryption Standard consists of the HMAC which is used to provide an authentication to the mobile users. In this application

SMS is send from one mobile to another mobile with high speed and the efficiency is also very high. The new protocol is used in this application [2].

Using Advanced Encryption Standard algorithm an author develop an application to secure the data between two communicating users. The AES algorithm consists of the Diffie Hellman algorithm. In this application an author used the Diffie Hellman algorithm to exchange the key between two users. Diffie Hellman algorithm is the most effective algorithm than the other algorithm [3].

C. Rivest Shamir Adleman Algorithm (RSA)

Rivest Shamir Adleman Algorithm is one of the most challenging algorithm. This algorithm is develop by the

Ron Rivest, Adi Shamir, and Len Adleman IN 1997.The RSA algorithm is one of the most widely used algorithm and the implementation of this algorithm is very simple as compared to the another algorithm. It consists of the encryption and decryption to encrypt and decrypt the data. The key size of the RSA algorithm is larger than the Elliptic Curve Cryptography. The RSA algorithm consists of the prime number and the product of the prime number forms the encryption key. This encryption is used to secure the data in the system [4].

In RSA algorithm consist of many operations. One of the most important operations is the modular exponentiation. By using this operation we can encrypt and decrypt the message. Many attacks are bombarded on the RSA algorithm and these attacks are hold successful against the RSA algorithm. The RSA algorithm having the block cipher scheme [5].

RSA algorithm is used to encrypt and decrypt the data on A secure extensible and efficient SMS application is develop using the RSA algorithm. Using this application two users can transfer the encrypted message to each other. All the procedure takes some time to exchange the message between two users. We can achieve the better performance by adding some random delay to the algorithm [8].

D .Elliptic Curve Cryptography

Elliptic curve cryptography is one of the most important cryptography and is more secure than the other cryptography. Elliptic curve cryptography consists of the mathematical bore. Elliptic curve cryptography consists of various operations. One of the most important operations is the addition operation .In the elliptic curve cryptography multiple addition is the identical part of cryptography. The key size in Elliptic curve cryptography is 256 bits. Elliptic key cryptography contains the various techniques, the most important and high speed technique is the pollard rho technique. The elliptic curve cryptography contains the smaller key as compared to the other cryptography and this is the advantages of the Elliptic Curve Cryptography

Author has proposed an evaluation technique on the basis of the encryption and decryption. In this system author explain a whole encryption technique. Firstly the message is in the plaintext form and this message is encrypted using any key and then send the message and lastly the receiver decrypt the message using any key. Either the key is symmetric key or asymmetric key [9].

VI. PROPOSED SYSTEM

In proposed solution we provide a framework for secure end to end mobile banking. For this purpose we used symmetric encryption algorithm for encryption purpose we used MAES encryption algorithm. To make mobile banking first mobile user registers their mobile number to the respected bank. Bank verifies the detail of customer and to save the mobile number in the bank database and gives secure key to the customer in the format of SMS or in the letter or mail secure key to the respected customer email id. These secure key is stored in encrypted format in the database. Bank provide mobile application that is install in mobile handset for secure mobile banking that encrypt and decrypt the message and provide end to end security of message . The Secure message contain mobile id, MAC, encrypted message and transaction time .the client send its mobile id, MAC1 ,encrypted message will beGenerated using modified AES symmetric encryption algorithm and transaction time is at the time request will be generated these all contain are send to the bank server. Server decrypt the message

and calculate MAC1' and check MAC1'=MAC1 and check mobile id if it is correct then it generate one time password (OTP) encrypted using MAES algorithm. These OTP are stored into the database .The server send MAC2, E (OTP), and transaction time all these contain are send to the client. Client calculate MAC2' and check MAC2'=MAC2 if it is found correct then it send back replay with OTP and transaction time to the server. Server check the OTP with stored OTP if it is found correct then authentication of client is successful.

There are four main security constraints that can be maintained by any framework or protocol. The four constraints are confidentiality, integrity, non-repudiation, and authentication. The proposed solution will be maintain all the four security constraint confidentiality of the SMS will be maintain using symmetric encryption algorithm and integrity will be maintain using hash algorithm i.e. MAC that can check hash function and will be maintain integrity of the message. Non-repudiation will be maintain using one time password and Authentication will be done using various authentication pattern like account number, Secret key and one time password.

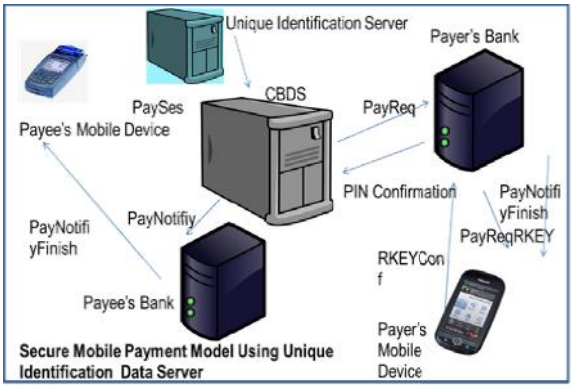


Fig. Proposed Architecture Diagram for Security service

VII. SMS GATEWAY ARCHITECTURE

SMS gateway is a powerful, flexible SMS Gateway application that enables the applications to send/receive SMS messages to mobile devices with your computer. It has an easy to use user interface, and an excellent internal architecture. The application can use a GSM mobile phone attached to the PC with a phone-to-PC data cable or IP SMS technology to transmit and receive the messages. Message Server works on Microsoft Windows XP, 2000, 2003 operating systems. Office users can use Microsoft Outlook, Microsoft Outlook Express and Microsoft Excel to send hundreds of messages to their clients. The messages and the phone numbers are stored in Excel files and an Excel Macro initiates the sending process. (The excel macro is included in the software package.) Software developers can integrate SMS messaging functionality into their applications very easily. For example if an SMS message needs to be sent, it can be inserted into a database table used for outgoing messages. The Message Server monitors this table and delivers the message. The Message Server puts all received SMS in another database table used for incoming messages. Of course many other APIs are available in the software to support software development.

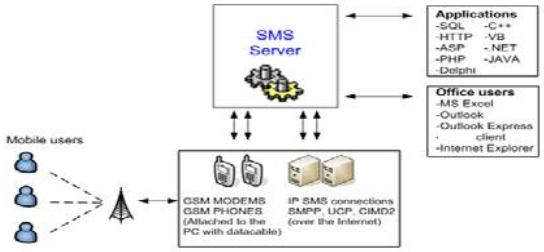


Fig. SMS gateway system architecture

VIII. CONCLUSION

Secured Messenger application is successfully designed in order to provide end to end secure communication through SMS between mobile users. The analysis of the proposed system shows that this system is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the proposed system. This system utilizes bandwidth efficiently. . This system contains a high security authentication mechanism, which confirms true identities can generate the 128 bit session key. And it also ensures message integrity and confidentiality.We have implemented a framework that provides secure mobile transaction using mobile banking application. All messages are sent from customer in encrypted format, bank decrypt the message and process the query and send response in encrypted format to the mobile .user decrypt this message using the banking application install in

mobile. In the future work we analyze the encryption algorithm which is better than AES, we can use concept of SIM application toolkit where bank store application and encryption key on SIM

FUTURE SCOPE

In the future, for security of SMS various kinds of latest encryption algorithms and the hash functions are yet to be analyzed. We will try to integrate the channel coding and the encryption procedure so that it will give errorless secures fastest SMS transmission. The application could also provide multiple senders ID implementation. The other desktop application could alsoport to different programming platform. There could also provide various mobile applications.

REFERENCES

[1] NeeteshSaxena ,Narendra S. Chaudhary EasySMS: A Protocol For End-to-End Secure Trans-mission Of SMS IEEE Transactions On Information Forensics And Security, Vol. 9, No. 7,July 2014

[2] Geovandro C C.C.Pereira,MateusA.S.Santos ,Bruno T. De Oliveira SMSCrypto: A lightweight cryptographic framework for secure SMS transmission The Journal of Systems and Software 86 (2013) 698 706

[3] Nikhil Sakhare, MithilWasnik Secure System Of Short Message Service (SMS) For GSM Networks International Journal of Soft Computing and Arti_cial Intelligence, ISSN: 2321- 404X Nov 2013

[4] SSMS Mohsen Toorani, Ali AsgharBeheshtiShiraziA Secure SMS Messaging Protocol for the M-Payment Systems IEEE 2008

[5] L.-C. Lo, J. Bishop, and J. H. Elo_, SMSSec: an end-to-end protocol for secure SMS Computers and Security vol. 27, 2008, 154-167

[6] H. Zhao and S. Muftic, Design and implementation of a mobile transactions client system:Secure UICC mobile wallet, International Journal for Information Security Research, vol. 1,2011, 113-120

[7] H. Harb, H. Farahat, and M. Ezz, SecureSMSPay: secure SMS mobile payment model, Proc.2nd International Conference on Anti-counterfeiting, Security and Identi_cation, 2008. ASID,2008

[8] H. Mathkour, G. Assassa, A. Al-Muharib, and A. Jumah, A Secured Cryptographic Messaging System Proc. International Conference on Machine Learning and Computing (ICMLC), 2009

[9] N. Saxena and N. S. Chaudhari, Secure encryption with digital signature approach for Short Message Service, Proc. World Congress on Information and Communication Technologies (WICT), 2012

[10] M. Hassinen, Java based public key infrastructure for sms messaging, Proc. 2nd International Conference on Information and Communication Technologies, 2006. ICTTA06, 2006, 88-93

Authors

Sai Dharma Reddy Gudimetlafrom GayatriVidyaParishad College of Engineering (A).securepayments (Android Devloper) Gachibowli,Hyderabad. His ResearchInterestsare - android security, mobile payments

BuddharajuShanmukhVarma from GayatriVidyaParishad College of Engineering (A). Areas of research interest include Android, Software testing, mobile payments.

SaiRaghukanth Reddy Gudimetla from GayatriVidyaParishad College of Engineering (A).Areas of research interest include Android, Software testing, mobile payments