International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1	**VOL**	02
Website	icssccet.org	**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016	**Accepted**	10 - March – 2016
Article ID	ICSSCCET053	**eAID**	ICSSCCET.2016.053

Mobile Application for Secured Message Transmission using MD5 Algorithm

K Kalaiselvi[1], B Hanuviyas[2], R P Pravin[3], T Renuka[4], R Saranya[5]
[1]Faculty CSE, [2,3,4,5] Final Year B.E CSE, Karpagam Institute of Technology, Coimbatore.

Abstract: *Short Message Service (SMS) has become one of the high speed and rugged communication channels to transmit the information across the worldwide. Sometimes, we send the confidential information like password, pass code, banking details and domestic identity to our friends, family members and service providers via SMS. SMS messages are dispatched as plaintext among mobile user (MS) and the SMS centre (SMSC), using wireless network. SMS contents are stored in the systems of the network operators and can be read by their personnel. Since, the SMS is sent as plaintext, thus network operators can easily retrieve the content of SMS during the conveyance at SMSC. So the long-established SMS service put forward by various mobile operators surprisingly does not furnish information security of the message being conveyed over the network. In order to secure such confidential information, it is forcefully required to contribute secure communication between end users. The above requirements can be accomplished by proposing a protocol called Cipher-SMS which provides end-to-end security during the dispatch of SMS over the network. The Cipher-SMS protocol achieved by using cryptographic algorithms of AES and MD5, The Cipher-SMS protocol intercepts the SMS information from various attacks including SMS disclosure, over the air (OTA) refinement, replay attack, man-in-the-middle attack, and impersonation attack. Proposed SMS based framework offers a low-bandwidth, reliable, efficient and cost effective solution for SMS Transmission. Cipher-SMS is the first protocol wholly based on the symmetric key cryptography of AES and hash cryptography of MD5 for cellular network.*

Keywords: SMS-Short Message Service, AES-Advanced Encryption System, MD5-Message Digest Algorithm, MS-Mobile Station

I.INTRODUCTION

Existing System

- SMS which provides secure communication through SMS between end users. SMS is executed which makes available the symmetric shared key among both MS and then ciphering of message takes place using a symmetric key algorithm. The working of the protocol is awarded by considering two different scenarios are SMS Sec and PK-SIM protocols.
- SMS Sec protocol can be used to secure an SMS communication dispatched by Java's Wireless Messaging API while the PK-SIM protocol proposes a standard SIM card accompanied by additional PKI functionality. Both protocols are based on client-server paradigm.
- In SMS protocol, a cryptographic encryption algorithm AES/MAES is maintained to provide end-to-end confidentiality to the transmitted SMS in the network.

Limitations / Disadvantages

- SMS grants SMS security with symmetric key cryptography, the existing protocol is wholly based on symmetric key cryptography.

Cite this article as: K Kalaiselvi, B Hanuviyas, R P Pravin, T Renuka, R Saranya. "Mobile Application for Secured Message Transmission using MD5 Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 286-290. Print.

- The dispatch of symmetric key to the mobile users is efficiently managed by the protocol.
- Security loses when hacking key transmission among Mobile Station.

Proposed System

- The Cipher-SMS offers end-to-end security during the dispatch of SMS over the network. The Cipher-SMS protocol obtained by using cryptographic algorithms of AES and MD5.
- The Cipher-SMS protocol arrests the SMS information from numerous attacks including SMS disclosure, over the air (OTA) refinement, replay attack, man-in-the-middle attack, and impersonation attack.
- Proposed Message Service based framework gives a low-bandwidth, reliable, efficient and cost effective solution for SMS Dispatchment. Cipher-SMS is the first protocol wholly based on the symmetric key cryptography of AES and hash cryptography of MD5 for cellular network.
- This Cipher-SMS shoots lower number of transmitted bits generates less computation overhead, and decrements bandwidth consumption and message exchanged as compare to existing protocols.

Advantages

- This protocol produces fewer communication and computation overheads, utilizes bandwidth efficiently, and decreases message exchanged during authentication than SMS (existing) protocols.
- Here preferred a symmetric key algorithm of AES with MD5 because these algorithms are 1000 times highly faster than the asymmetric algorithms and enhances the efficiency of the system.
- Achieved more security than SMS by utilizing AES with MD5 algorithms.
- No use when Hacking AES key among Mobile Stations, because MD5 generates different key ID of each dispatchment.

II. Encryption Based Channel Coding Algorithm for Secure SMS

SMS has a miscellany of benifits and drawbacks for M-Commerce purpose. The advantages are it is easy to use, a common messaging tool in the middle of consumers, works across all wireless operators, affordable for mobile users, no specific software required for setting up, allows banks and financial institutions to provide real-time information to consumers and employees and stocked messages can be contacted without a network connection. Most important disadvantage of SMS is that it don't offer a tenacious environment for confidential data during transmission and there is no standard manoeuvre to certify the SMS sender. There is a necessity for an end to end SMS Encryption with errorless message transmission in order to provide a impregnable with error free data transmission for communication. These two factors are important for SMS. We have analyzed about mainly JCCC and Soft Input Decryption (SID). We proposed a novel theoretically scheme NTRU Sign algorithm. We are expect that it will improve the current security level speed and provide reliable message at receiver end.

III. The Implementation of Security Message Protocol for PDA PUSH Service

We contemplated and implement a service model to delegate messages safely for PDA on CDMA wireless networks and a secure message transfer etiquette which considers physiognomy of PDA. The contemplated PUSH service uses SMS (short message service) to connect an offline applicant device with the wired network for data communication. After receiving SMS message, client device handle the SMS missive and creates a data channel through RAS (remote access service), and then the data of the server can be strapped to client. The implemented impregnable etiquette can provide safe data transmission on each communication channel through two way channels of SMS and data. This etiquette can reduce a number of conveyances for exchanging a safe session key by using surveillance nonce table. As a result, intensity of encryption can be increased.

IV. High Security Communication Protocol for SMS

Nowadays, short message service (SMS) is encrusted with various security threats. Thus, the fields of high covertness (e.g., mobile E-commerce) require a higher level of protection on SMS. Secure communication in incredible mobile network has very important connotation. This paper presents a high security communication protocol for SMS. Through corroboration, decryption and integrity aegis, it authorise an end-to-end secure channel between server-side and mobile boundary. Through reviewed it by svo logic, this etiquette is proved to ensure confidentiality, integrity and non-repudiation of SMS messages.

V. Performance Evaluation on End-to-End Security Architecture for Mobile Banking System

The advantage of mobile dissemination enables mobile operators to provide value added service such as bulwarked mobile banking, mobile commerce and provide enriched security for internet banking. Mobile banking is attractive because it is a convenient tactic to

Cite this article as: K Kalaiselvi, B Hanuviyas, R P Pravin, T Renuka, R Saranya. "Mobile Application for Secured Message Transmission using MD5 Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 286-290. Print.

accomplish banking from anywhere any time, but there are security concerns in the implementation, which include glitches with GSM, network, SMS, GPRS etiquette. An end-to-end security framework using PKI for mobile banking is contemplated. Performance of the proposed model is presented.

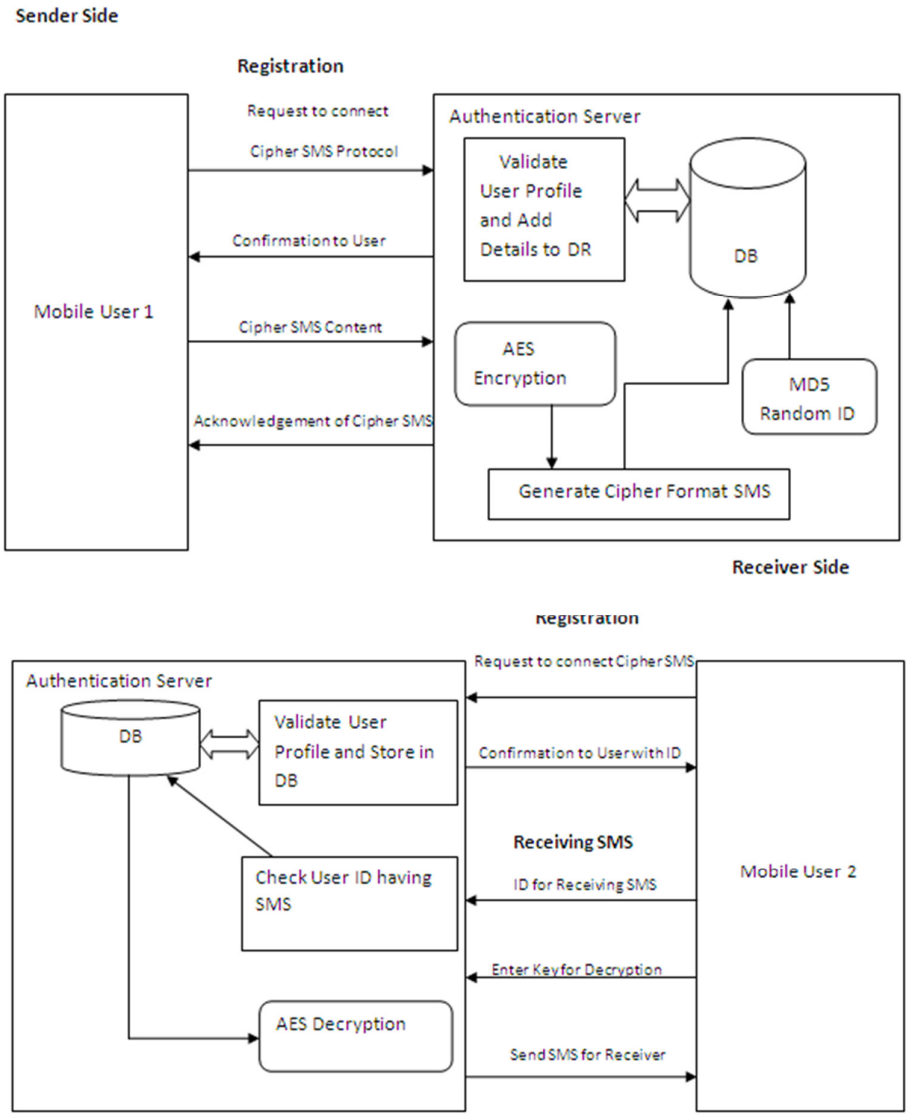
VI.A Secure Information Transmission Expedient with a Secret Key Based on Polar Coding

A new secure information transmission intrigue based on polar codes with a pre-shared classified key is proposed. In polar codes, after the channel divarication is induced, good split channels are used to impart the user message and bad channels are occupied to support the reconstruction of the message by sharing fixed data. If the fixed data in bad channels is classified, an adversary gets difficulty in improving the user message in good channels without knowledge of the fixed data. From this scrutiny, we construct a secure information transmission scheme. By appending pre-post-depuration that imposes a territory between the transmitted message sub-blocks, the adversary's complexity can be changed to an intractability, since only sectional information can be decodable by attackers. A new class of confidential key scheme is developed in such a way.

VII. Solution

Cipher-SMS protocol provides secure communication through SMS between mobile users by using AES and MD5 encryption.

VIII. Overview of the Project

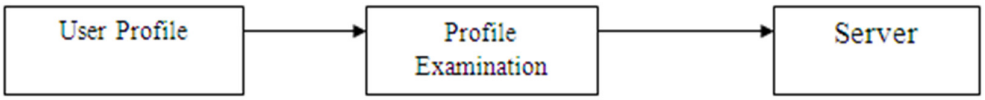


Cite this article as: K Kalaiselvi, B Hanuviyas, R P Pravin, T Renuka, R Saranya. "Mobile Application for Secured Message Transmission using MD5 Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 286-290. Print.

1. User Profile
2. SMS Communication
3. Authentication Server
4. Symmetric Key

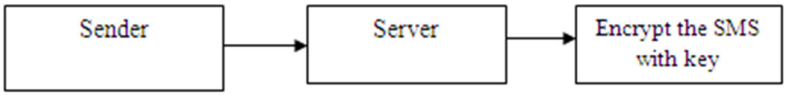
1. User Profile

The mobile device that apprehend the user details with some parameters, that recognize the authenticate user. This restricts the non-owner users to see information about the SMS we send. However, any mobile device using this facility can get some additional report examination has to be controlled with some unique parameter. Through this function, the mobile device can allow authenticated profile owner to access the data and send secure SMS to others.



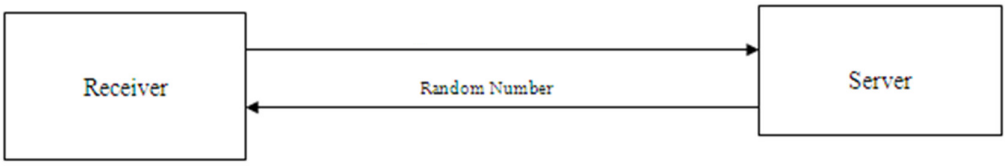
2. SMS Communication

The Authenticated mobile user can send the SMS with some key to the server. The mobile who wants to send SMS must be registered with server. The mobile sends the SMS with certain key to server. The server can encrypt the original message using AES algorithm and the send SMS to receiver through base station and mobile station



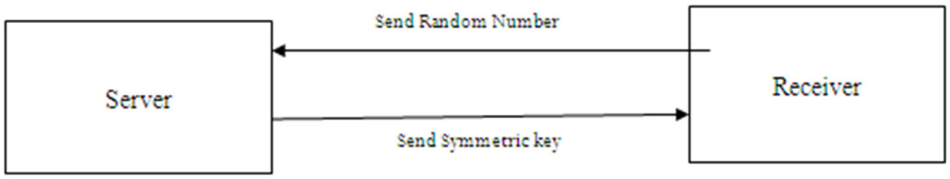
3. Authentication Server

The Encrypted message can travel through base station. Receiver receives the message in secure inbox. Now the receiver wants to unravels the message. So receiver requests the key using random number generator from server. Then server generates the random number and sends it to the receiver.



4. Symmetric KEY

Server recognizes the random number from receiver; from this server authenticate the authorized receiver. Then server proceeds the symmetric key to receiver. After getting symmetric key, receiver decrypts the encrypted message and extracts the original message in secure inbox.



IX. MD5 Algorithm

a. MD5 Logic

The algorithm takes as input a message of capricious length and produces as output a 128-bit message digest. The input is functioned in 512-bit blocks.

Cite this article as: K Kalaiselvi, B Hanuviyas, R P Pravin, T Renuka, R Saranya. "Mobile Application for Secured Message Transmission using MD5 Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 286-290. Print.

b. Working of MD5 Algorithm

- Append padding bit.
- Append length.
- Initialize MD buffer.
- Process message in 512-bit blocks (16 WORD).
- Output after processing nth stage is 128-bit message digest.

X. Conclusion and Future Work

Cipher SMS protocol is to provide end-to-end secure communication through SMS between mobile users. The analysis of the contemplated etiquette shows that the etiquette is able to prevent various attacks including SMS disclosure, over the air (OTA) alteration, replay attack, man-in-the-middle attack, and caricature attack. The transmission of symmetric key to the mobile users is efficiently managed by the etiquette. This etiquette produces lower communication and computation overheads, utilizes bandwidth dexterously, and reduces message exchanged during authentication than SMSSec and PK-SIM etiquette.

References

1. I. Murynets, R. Jover, "Crime Scene Investigation: SMS Spam Data Analysis," IMC, 2012, pp. 441-452.
2. K. Par, "Smartphone remote lock and wipe system with integrity checking of SMS notification," IEEE ICCE, 2011, pp. 263-264.
3. A. Nehra, R. Meena, "A robust approach to prevent software piracy," SCES, 2012, pp. 1-3.
4. N. Gligoric, T. Dimcic, D. Drajic, "Application layer security mechanism for M2M communication over SMS," TELFOR, 2012, pp. 5-8.
5. J. Lo, J. Bishop, J. Eloff (2008). SMSSec: An End-to-end Protocol for Secure SMS. *Computers & Security, 27(5-6), pp. 154–167.*
6. M. Hassinen, "Java based Public Key Infrastructure for SMS Messaging," ICTTA, 2006, pp. 88-93.

Cite this article as: K Kalaiselvi, B Hanuviyas, R P Pravin, T Renuka, R Saranya. "Mobile Application for Secured Message Transmission using MD5 Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 286-290. Print.