Indian Journal of Science and Technology, Vol 9(30), DOI: 10.17485/ijst/2016/v9i30/98718, August 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Securing Message at End-to-End Mobile Communication Using Cryptography Algorithm

K. Jaya Rohit, M. Siva Rama Krishna, C. H. Geetha Krishna and P. S. G. Aruna Sri*

Department of ECM, Koneru Lakshmaiah University, Vaddeswaram Village, Tadepali Mandal, Guntur District - 522502, Andhra Pradesh, India; rohitkovvuri@gmail.com, muppaneninani@gmail.com, geethuhoney9@gmail.com, arunasri_2012@kluniversity.in

Abstract

Background/Objectives: State the objectives of your work clearly. **Methods/Statistical Analysis:** State the methodology you employed to meet the objectives. **Findings:** Rewrite your findings. **Application/Improvements:** Here we are using mobile users and authentication server. Authentication server is uploaded with SQL server which help to store the user ID and password of the mobile users.

Keywords: Authentication Server, Cryptography, Decryption, Encryption, End-to-End Communication, Security

1. Introduction

SMS is one of the modes of sharing information including account number, pan card variety, debit card variety, license variety, credit card variety, banking details, debit card password, credit score card password etc. In such a case there is a need to use protocols such as easy SMS, Cipher SMS for encryption and decryption at authentication server. The encrypted message and decrypted message are saved inside the database of authentication server. If the database is loaded closely then there might be no chance to use the authentication server with the aid of any other cell user.[1]

To overcome the above trouble we're going to set up the encryption and decryption for mobile customers. So the encrypted statistics is send to another mobile user via their respective communication. The communication database will shop the encrypted records and ship to the vacation spot as cipher textual content. The apparent text become encrypted through the cellular person 1 and the cipher textual content is decrypted with the aid of the cell person 2.

Formerly, various authors reported specific protocols like smooth SMS, SMS sec, PK-SIM, and cipher SMS for presenting safety to the confidential data that's presented inside the message. Right here the easy SMS, SMS sec, PK-SIM and cipher SMS are the end-to-stop secure communication. SMS is being utilized in healthcare monitoring, cell banking, cell trade, transportation data machine. From the protocols smooth SMS, SMS sec, and PK-SIM and cipher SMS conquer the assaults inclusive of SMS disclosure, Over the Air amendment (OTA), reply assault, man in the middle attack, impersonation assault. Those protocols use the authentication for encrypting and decrypting the message, in which cipher SMS and clean SMS generates minimal communication and computation. Because of the minimum communication the easy SMS and cipher SMS produce 51% and 31% of the bandwidth consumption, 62% and 45% of the message change during the authentication.

If we don't forget cipher SMS protocol it affords the quit-to-give up safety during the transmission of the SMS over the communication. This cipher SMS sends lesser range of transmitted-bits, generate much less computation and reduce the bandwidth intake and message exchange.

The framework relaxed Extensible and efficient SMS (SEESMS) permits the peer to look verbal exchange with cipher text. on this framework we must do not forget the 2 cellular communications, for sending the message from one end to the opposite end.[2] Within the relaxed extensible

*Author for correspondence

and efficient SMS we are the usage of public key cryptography for replacing encrypted verbal exchange among peer to peer. The mobile user1 message which is encrypted by the authentication server using the general public key. The cellular user2 will get the message in encrypted form then cellular person ought to use the non-public key for the decrypting the records. In SEESMS we're going to public key cryptography to preserve privateness lots because it makes use of keys for changing the apparent text to the cipher textual content at cellular user1 we ought to use public key and for converting the cipher textual content to the plain textual content we ought to use non-public key.

The framework security brief Message service (SSMS) is allowing the SMS as a secure bearer for M-fee. Right here we're presenting safety to the message by means of the use of elliptic curve based public key. Elliptic curved based public key is the secret key established order at the quit customers. While the cellular is speaking with each different by using security short Message carrier the mobile user1 need to be use the elliptic curve based totally public key for converting the obvious text message to the cipher text message. If the cipher text is taken into consideration at cellular user2 then the message must convert the cipher text to straightforward textual content by means of using the elliptic curve based public key.[3] Security short Message service is provide an safety attribute in SMS by means of establishing mystery key.

SMS based framework presents a low-bandwidth, reliable, green and fee powerful solution for scientific records acquisition. It generate shared key for each consultation however additionally generate big overheads and no longer suitable for the real world packages. In all, it is not clear whether or not the proposed techniques are able to prevent SMS against diverse assaults. All of the above noted approaches/ protocols/ frameworks generate a big overhead as they propose a further framework for the security of SMS. Because of physical obstacles of the cellular phones, its miles endorsed to develop a protocol which might make minimum use of computing sources and could offer higher protection. But, implementation of framework continually will increase the general overhead which isn't always lots appropriate for the aid constraints devices which includes mobile telephones.[4]

Easy SMS, SMS sec, PK-SIM which does no longer endorse to change the present architecture of cellular communication. In clean SMS the mobile customers are verbal exchange two methods, by way of the usage of equal authentication server at cell users, and with the aid of using distinctive authentication server at mobile users.

While mobile users the usage of identical authentication server the cell user1 need to method the authentication server to offer protection to the message, first the mobile user1 ought to sign in with authentication server. While the cellular person is sign up with authentication server, the cellular user has to ship message then the authentication server must convert the message form plain textual content to the cipher text. The message which is encrypted it must be send to the cellular user2. The cell user2 additionally use the equal authentication server to transform the cipher text to straightforward textual content. While message is decrypting cellular user need to sign up with the authentication server, then the authentication sever is capable of convert the cipher text to the plain textual content.

While cell consumer the usage of exclusive authentication server the cell user1 have to method the authentication server to offer protection to the message, first the cell person must check in with the authentication server, the mobile person has to send message then the authentication server need to convert the message shape plain text to the cipher text. The message that is encrypted it need to be ship to the mobile user2. The cell user2 also use the any other authentication server to convert the cipher text to standard text. When message is decrypting cellular consumer need to sign up with the authentication server, then the authentication sever is capable of convert the cipher textual content to the apparent textual content.

SMS sec protocol may be used to relaxed SMS communication despatched by means of java Wi-Fi messaging API. PK-SIM protocol proposes a preferred SIM card with extra PKI capability. SMS sec and PK-SIM are based on customer-server application. Here the customer server application is described as arranging a cellular user at one aspect of the verbal exchange and arranging the authentication server at different aspect of the verbal exchange device. However there has been no relation in which SMS is despatched from one cell person to any other mobile person.

In clean SMS there are two members of the family to send SMS from one cell to every other cellular. If the cell user use the same authentication server for transmission of message is called as same home area sign up. If the mobile consumer use the distinctive authentication server for transmission of message is called as one of a

kind domestic region check in. Authentication server is used for storing the symmetric key or uneven key that is shared among authentication server and the respective mobile users.

Cipher SMS is result for the imparting top cellular network while examine to smooth SMS as it affords the registration authority with licensed, it assist to constructed a cell network between mobiles and stores all of the records related to cellular subscriber.[5]

As soon as the cellular customers proportion the secret key, then there might be feasible to exchange the message from plain textual content to cipher text in addition to cipher text to the obvious text. formerly authors use enhance Encryption preferred for changing the obvious textual content to cipher text at the authentication server as well as the cipher text of the message is converted via the opposite stop the usage of identical AES algorithm.

When we compare with easy SMS, Cipher SMS, SMS sec Protocol, PK-SIM protocol, all of them are save the big records at authentication server. Now we are introducing a mechanism were authentication does now not have hassle at database. Right here we are going to get entry to the authentication server for key era cause but no longer encrypting and decrypting the records at authentication server.

2. Proposed Solution

Right here we are considering two mobile users to access the authentication server. The authentication server provides 16-character secret key for encrypting the data and decrypting data of the mobile users.

2.1 Authentication Server

In authentication server the sixteen-character mystery key installed. To get right of entry to the secret key cellular consumer must register with the authentication server. Authentication server includes database which performs an essential role for gaining access to the consumer. Mobile users ought to sign up with their own consumer identification and password. One's consumer IDs and passwords are saved inside the database permanently. Here we are the use of 'sign up' and 'sign up' two keywords were sign in is used for the conformation with database and join up is used for the registration of recent consumer with authentication server. While the cellular customers want to get entry to the 16-character secret key beneath steps has to comply with.

- Any cell consumer first has to sign up with their user id and password. If the mobile person didn't have any consumer identity the authentication server will not respond.
- Authentication server will react when the mobile user sign in with their user identification and password efficaciously.
- While the mobile user is register with their user identification and password the database will verify the each. If any individual of them isn't always correct the 16-character secret key will not get entry to.
- When the mobile consumer is check in with their person id and password the database will verify the each. If anybody of them is accurate the 16- character secret key will get right of entry to.

Authentication server (Figure 1) is used for getting access to the 16- character secret key but no longer encrypting the information and decrypting the records. Database is stored simplest the person identification and passwords of the cellular users but they do no longer keep the encrypted facts and decrypted records.

Authentication server will take three situations when the cellular consumer request is accessed: First one is if the mobile consumer identity isn't identical to the database identification (user id no longer identical DB id) and password of the cell person is equal to database password (person PW equal DB PW). Second one is that if the cellular person id is equal to the database identification (person id identical DB id) and password of the mobile user isn't always same to database password (user PW no longer equal DB PW). Third one is if the mobile consumer identity isn't equal to the database id (person identity not identical DB identification) and password of the cell person isn't identical to database password (user PW now not equal DB PW). Underneath flow chart (Figure 2) will pro-

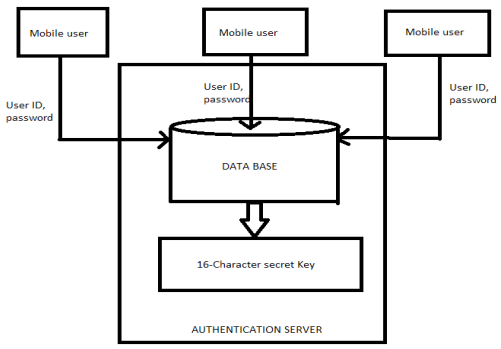

Figure 1. Authentication server.

vide an explanation for the access of authentication server by the cell consumer.

2.2 Generating 16-Character Secret Key

When mobile user get right of entry to the authentication server the 16-character secret key is generated. It is generated via the use of the superior Encryption preferred which has the capability to generate the 16-character secret key.[6]

Advanced Encryption trendy is also suitable to generate the 24-character secret key and 32-character secret key due to the fact its minimum block size is 126 bits (sixteen-characters) and maximum block size is 256 bits (32-characters). However we're thinking about sixteen-person secret key because it is straight forward to recognize the process of generating key at authentication server.

In 16- character secret key there are 4 modules: Sub Bytes, Shift Rows, mix columns, upload spherical key. While these four modules perform ten rounds then sixteen-individual secret keys generated.

2.2.1 Sub Byte Module

When the mobile user access the database then it will approach to the 16-character secret key module one is Sub Byte. First we initially built a 16-charactet matrix or 4*4 matrix.

Know we will introduce an s-box substitution step, which will replace the each character in the 16-character matrix. This step causes confusion of data in the matrix.

2.2.2 Shift Rows Module

When the Sub Byte step is completed, the result of Sub Byte is the input to the shift row. This operation performed on the rows of the matrix which generated by the Sub Byte. When we considering the 16-character matrix the Shift Row perform on the rows as follow:

- First row of the matrix does not change its position. The four characters which are in first row will be same as the first row of the Sub Byte Matrix result.
- Second Row of the matrix performs one position shift to the left. The four character which are in the second row differ with one position when compare with Sub Byte Matrix Result.
- Third Row of the matrix performs two position shifts to the left. The four character which are in the second row differ with two positions when compare with Sub Byte Matrix Result.
- Fourth Row of the matrix performs three position shifts to the left. The four character which are in the second row differ with three positions when compare with Sub Byte Matrix Result.

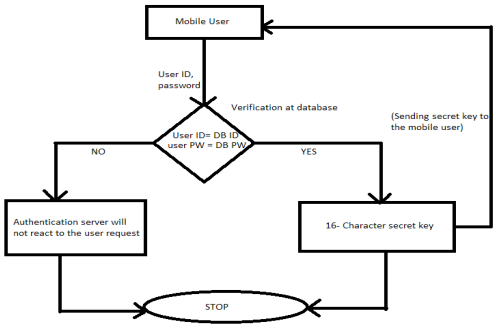

Figure 2. Flow chart for accessing the authentication server by mobile user.

2.2.3 Mix Columns Module

When Shift Row operation is completed, the result of Shift Row is the input to the Mix Column. The four characters of each column of the shift row matrix are combined with the polynomial 4*4 matrix which is randomly arranged.

Each column of the shift row matrix result is combined with polynomial matrix by using EX-OR operation. When EX-OR operation is performed the output is uploaded on the same column of the input matrix.

2.2.4 Add Round Key

When applying the various operations like Sub Byte, Shift Row, Shift Column on the initial matrix is called state matrix. State matrix is the input to add round key. Add round key is used for generate the new round key for every ten rounds. The new round key is generated by applying XOR-operation on the state matrix of particular round and initial matrix. After completing the ten rounds the 16-character secret key is generated.[7]

2.3 Encrypting the Data at Mobile user

Previously the sender will send the message to the authentication server for encryption. Authentication server will send the encrypted message and sender id to the receiver. The receiver will send the user id of the sender to the authentication server then it will ask for secret which is already shared between the sender and

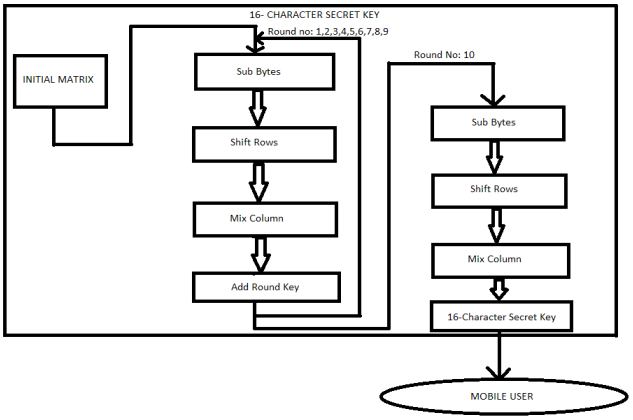

Figure 3. Architecture for generating 16- character secret key.

receiver. Authentication server will decrypt the data and send to the receiver. Here the database of the authentication server will loaded heavily. To overcome this problem we are going to encrypt the data at mobile users.

Mobile user has to register or sing up with authentication server. Users want to upload their password and user ID in the database of the authentication server because it will provide the security to the authentication server, database, and 16-character secret key. The steps followed to encrypt the data.

- Mobile user must sign in with the authentication server to verify in the database whether mobile user is member of the authentication server.
- The mobile user has to enter the mobile number of receiver and message before accessing the authentication server.
- If the mobile user is access with the authentication server then 16- character secret key is generated in the mobile automatically.
- Message which is typed by the user will combine with 16-character secret key and provides an output as encrypted message.
- Encrypted message will send to the receiver (Figure 4).

2.4 Decrypting the Data at Mobile user

Mobile user has to register or sing up with authentication server. Users want to upload their password and user ID in the database of the authentication server because it will provide the security to the authentication server, database, and 16-character secret key. The steps followed to decrypt the data.

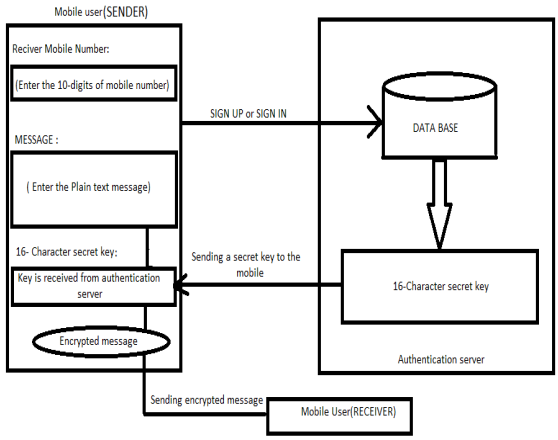

Figure 4. Encrypting the message by mobile user using authentication server.

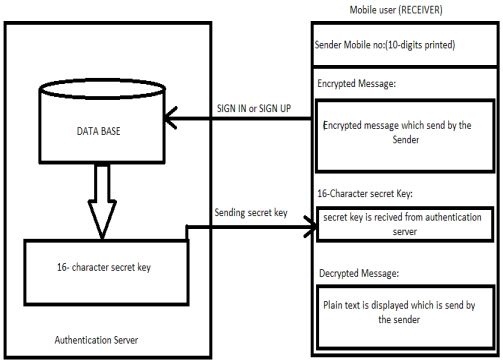

Figure 5. Decrypting the message at mobile user using authentication server.

- Mobile user will receive the message from sender which is in the encrypted form.
- When the message is received the mobile user has to sign in with the authentication server which sender has used.
- Mobile user must sign in with the authentication server to verify in the database whether mobile user is member of the authentication server.
- If the mobile user is access with the authentication server then 16- character secret key is generated in the mobile automatically.
- Message which is received by the receiver will automatically decrypted in the mobile by using 16- Character Secret Key.
- Finally the result is in decrypted form which is able to read by the user.(Figure 5)

3. Conclusion

When we are converting the message from plain text to cipher text (or) cipher text to plain text in mobile, the message is stored in mobile while it may be plain text or cipher text. Database of the authentication server have lot memory space when encryption and decryption is done at mobiles and able to store the sign up data. The number of mobile users will sign in the authentication server for getting 16-character secret key. When the memory space is huge then there will be access of number of mobile users

4. References

1. Agrawal V, Agrawal S, Deshmukh R. Analysis and Review of Encryption and Decryption for Secure Communication . International Journal of Scientific Engineering and Research (IJSER). 2014 Feb; 2(2):1–3.
2. Rayarikar R, Upadhyay S, Pimpale P. SMS Encryption using AES Algorithm on Android. International Journal of Computer Applications. 2012 Jul ; 50(19):1–6.
3. Rajanbabu DT, Raj C. Multi-Level Encryption and Decryption Tool for Secure Administrator Login over the Network. Indian Journal of Science and Technology. 2014 Apr; 7(S4):8–14.
4. Agrawal H, Sharma M. Implementation and analysis of various symmetric cryptosystems. Indian Journal of Science and Technology . 2010 Dec; 3(12):1–4.
5. Saxena N, Chaudhari NS. Easy SMS: A Protocol For End-to-End Secure Transmission. IEEE Transaction on Information Forensics and Security. 2014 Apr; 9(7):1157–68.
6. Srisai MT. Cipher SMS For End-to-End Secure Transmission of SMS. Proceedings of 9th IRF International Conference. 2015 Dec. p. 12–5.
7. Park K, Ma GI, Yi JH, Cho Y, Cho S, Park S. Smartphone remote lock and wipe system with integrity checking of SMS notification. Proc IEEE ICCE. 2011 Jan; 263–4.