ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Enhancing Security using Location of Mobile Users

Aniruddha S. Raut[1], Harshraj N. Shinde[2], Shubham R. Vidhale[3], Rohit V. Sawant[4], Vijay A. Kotkar[5]

Student, Department of Computer, AISSMS College of Engineering, Pune, Maharashtra, India[1234]

Assistant Professor, Department of Computer, AISSMS College of Engineering, Pune, Maharashtra, India[5]

ABSTRACT: Now-a-days, mobile phones are more powerful than what a desktop used to be few decades back. A hand held device or mobile phones are capable of performing operations what a desktop can perform. Many day-to-day operations are carried out by mobile phones but the most important is exchanging of confidential data such as documents, images etc., this needs to be encrypted. But only encryption of data is not enough in today's world. In this paper, we propose a solution that can enhance the security feature of an encryption algorithm using the real time location of a mobile user.

KEYWORDS: DES, 3DES, AES, encryption, decryption.

I. INTRODUCTION

Today's smart phones are powerful and compact in size; hence its growth rate has gone up exponentially. Due to ease of accessibility and different functions available in mobile phone, it has become an integral part of human life, be it social networking, shopping or exchanging of information between users. Hence, a sense of protectiveness arises for the data to be sent. There are many encryption algorithms available to encrypt your data. But only encryption algorithm is not enough. In this paper we are proposing a solution to enhance the security of an encryption algorithm using the Global Positioning System (GPS) for tracking the location of a mobile phone. In solution, we suggest that an encrypted file can only be decrypted by being at a particular location, which would be decided by the user who would be encrypting the file.

Encryption is the process of converting the plain text into a text which makes no sense to humans unless it is decrypted. The text which is encrypted is known as cipher text. For conversion of normal plain text to cipher text, a key is required. Let us take a simple example; "WORK" is a plain text which when shifted by 3 letters making '3' as a key, gives us the "ZQTM" as the cipher text [1].

II. RELATED WORK

Hsien-Chao et al showed a method where location is extracted from the mobile in coordinates of east and north then it is multiplied by 1000 and divided by Tolerance distance (TD) due to in accuracy of G.P.S. Then bitwise EX-ORing is done and using MD5 hash algorithm 128 bits key is generated which is divided in 64 bits which is known as LDEA keys. The key generated randomly which has same length as that of LDEA key, i.e. 64-bits. LDEA keys are then EX-OR'ed with randomly generated key (R) separately and final keys are generated and this generated keys are used for encryption process. When receiver gets the encrypted file with TD and R-key transmitted via symmetric algorithm. The application will acquire the location from GPS sensor, which will divided by TD and operated under MD5 hash algorithm followed by combining with R-key. At the end of this operations we will get final key with which we can decrypt the text [2].

Prasad reddy et al showed that on client side destinations latitude/longitude co-ordinate are given using this coordinates an LDEA key is obtained. This key is used for the encryption of given data. For providing more security R-key is also included in LDEA key. Rotationof bits of cipher text depends on the R- key after whitening(i.e. a decorrelationtransformation that transform a set of random variable having a known covariance matrix M into a set of new random variable whose covariance is the identity matrix) with the LDEA key using the Exclusive – OR operation.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

After the encryption of given data ,on the receiver side ,if the receiver is receiving the exact coordinate using GPS, then the receiver can decrypt the file using that coordinate [3].
Ayesha khan et al showed that the latitude and the longitude location positions of both (sender and receiver) is checked and then only the message will be decrypted. For e.g. If the sender is at (x,y) location and the receiver is at (a,b) location then using a hash function convert the values of (x,y) and (a,b) into an integer and multiply it with the RSA formula for encryption [4].

III. METHODOLOGY

A. Data Encryption Standard (DES):

DES is a block cipher which encrypts the data according to block of 64-bit. In this mechanism, 64-bit key is used for encrypting the plain text but each byte of it has 1-bit as parity bit, hence actual key length is 56-bit.DES consists of two fundamental functions of cryptography viz. substitution and transposition [5].

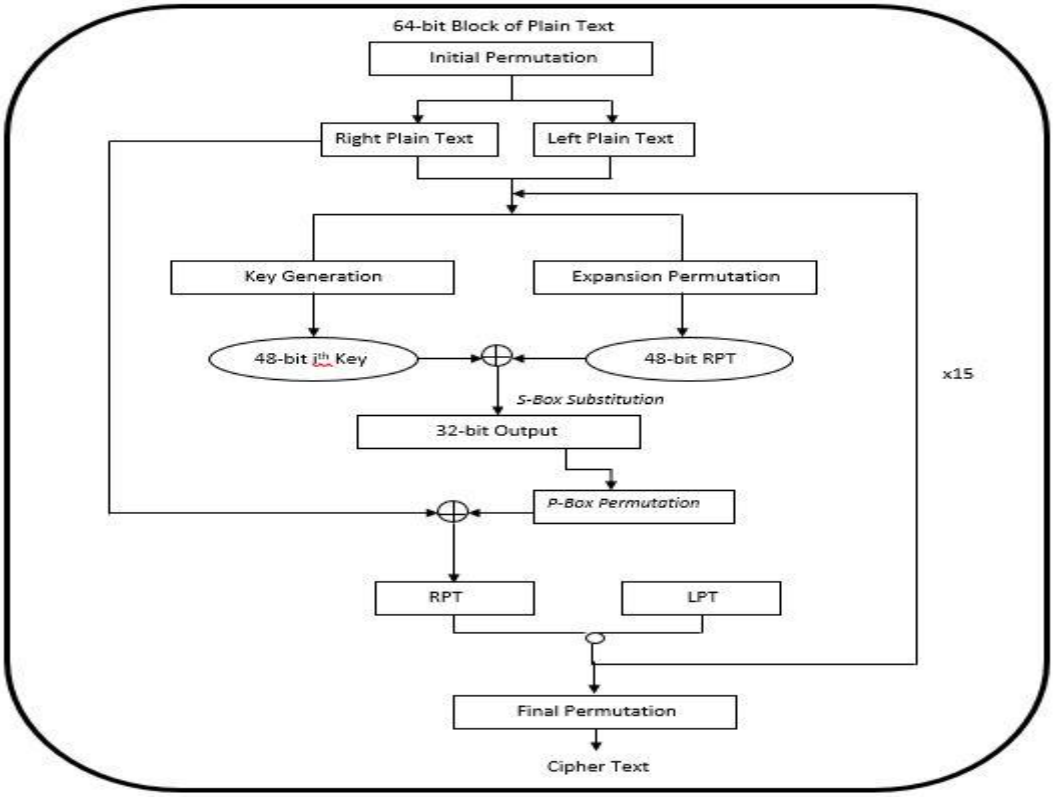


Fig. 1 DES flow diagram

The Fig. 1 shows the flow of DES. The steps shown in the figure are explained below:-
It consists of 16 rounds and several steps which are as follows:-

1. A block of 64-bit plain text is given to Initial Permutation.
2. Output of Initial Permutation gives two halves of permuted block.
   - Left Plain Text (LPT)
   - Right Plain Text (RPT)
3. Now LPT and RPT go through 16 rounds of encryption process each of which having its own generatedkey.

i. By using key transformation, 48-bit key is generated from 56-bit actualkey.
ii. RPT of 32-bit is expanded to 48-bit using Expansion Permutation.
iii. RPT expanded in prior step is EX-ORed with key.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

iv. Output got from prior step which is of 48-bit is reduced to 32-bit using S-Box substitution and output is permuted using P-Box permutation.
v. The P-box output is EX-ORed with LPT (32-bit) and result is stored in suppose temp.
vi. RPT becomes LPT and tempis stored in RPT for the next round.

Six steps described above are repeated 15 times.
Final Permutation is performed after completion of 16 rounds [6].

B. Triple Data Encryption Standard (3DES):

3DESis similar to DES only the difference is that in 3DES, DES is performed thrice.To overcome the drawbacks of DES i.e. brute force attack, weak keys and key space size, 3DES was introduced. In 3DES, DES algorithm is repeated three times using three keys. The keys may be different or same depending on the type being used.

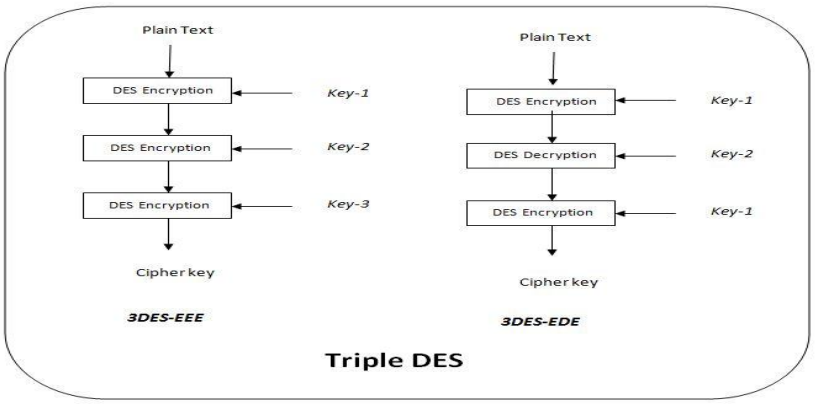


Fig. 2 Triple DES flow diagram

The Fig. 2 shows how the DES encryption is used thrice using different keys. Different types are there of 3DES some which is showed in the diagram and a brief explanation is given below.
Types of 3DES are as follows:-

i. 3DES-EEE: - Three DES encryptions are performed using three different keys.
ii. 3DES-EDE2:- Two DES encryption along with DES decryption in between i.e. encryption then decryption then again encryption is performed using two keys, same key is used for first and third operation [7].

C. Advanced Encryption Standard (AES):

In the late 1990s, the U.S. National Institute of Standards and Technology (NIST) conducted a competition to develop a replacement for DES. The winner, announced in 2001, is the Rijndael (pronounced "rhine-doll") algorithm, destined to become the new Advanced Encryption Standard [8]. AES uses symmetric key and is a block cipher, it divides the plain text in number of fixed size blocks and then encrypts it. Decryption is also block by block process.

AES algorithm takes 128 bit plain text and produces a 128 bit cipher text using a key. Usually, 128 bit key is used but they may vary according to requirement. Different keys available are 192 and 256 bit keys. Numbers of rounds are performed for encrypting a block i.e. a single block is encrypted number of times before sending.

Algorithm	Key Length	Block size	Number of rounds
AES-128	128 bits	4 words(16 bytes)	10
AES-192	192 bits	4 words(16 bytes)	12
AES-256	256 bits	4 words(16 bytes)	14

Table1: Key length and number of rounds

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

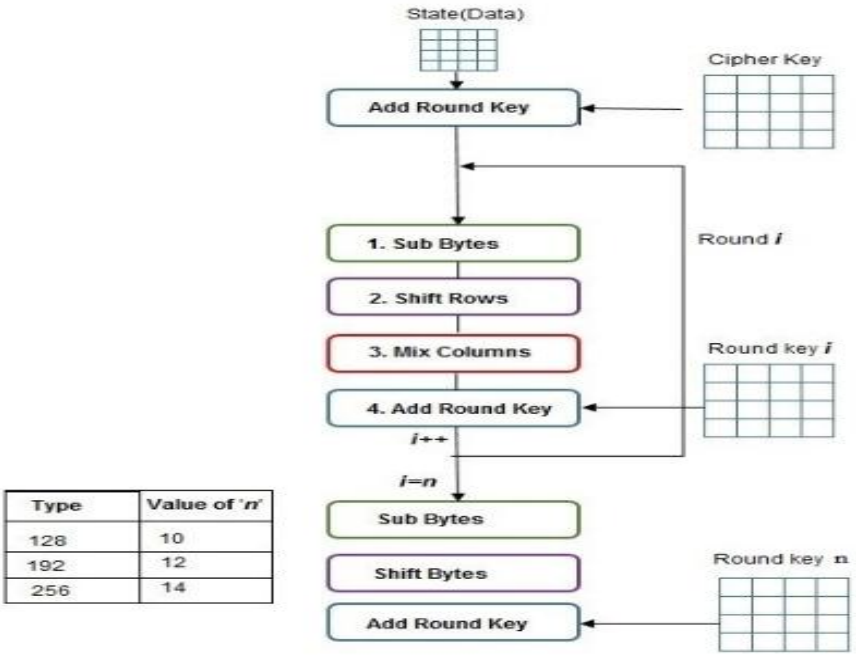
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

For different keys, different numbers of rounds are used. Table 1 shows different keys and their associated number of rounds and block size [9].

Working of AES:
The flow diagram of AES is as shown in Fig. 3 below and each function is explained briefly accordingly.



Type	Value of '*n*'
128	10
192	12
256	14

Fig. 3 Flow of AES

State array is the data which is to be encrypted. The data to be encrypted is converted into the hexadecimal and arranged in the matrix form. The size of matrix is 16 bytes. Number of such blocks is made according to the total size of data. As shown in Fig. 3, initially the key is directly XOR'ed with the state arrayand later, for each round the key is updated and then XOR'ed.Numbers of rounds are done according to the key length and different operations are done on state array. For the last round, mix-column has been excluded [10].

Working of each operation is explained briefly below:
Add round key: It is basically a XOR operation between key and state array. Initially, the original key is directly XOR'ed with state array and later, the key is updated for each round and then it is XOR'ed. An illustration is shown below in Fig. 4.

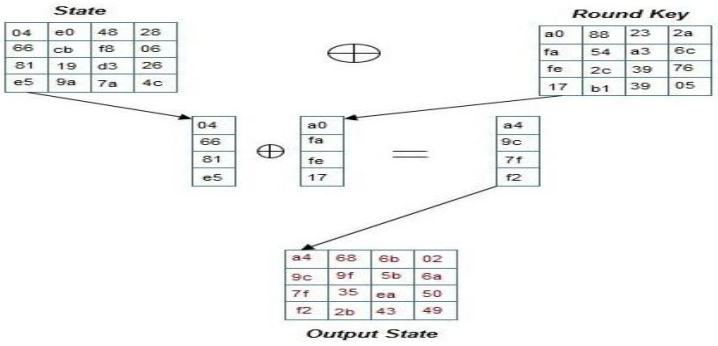


Fig. 4 Add round key

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

As shown in Fig. 4, first column is taken from both state arrays and keys areXOR'ed and which becomes first column of new state array.Same thing is done for all the columns and then the new state array is passed on to the later stages.

Sub Bytes: This is basically a substitution operation. In this operation, the data in the state array is replaced with hexadecimal given in the S-box. S-box is standard substitution box which is pre-defined for AES algorithm. An illustration is shown below in Fig. 5.

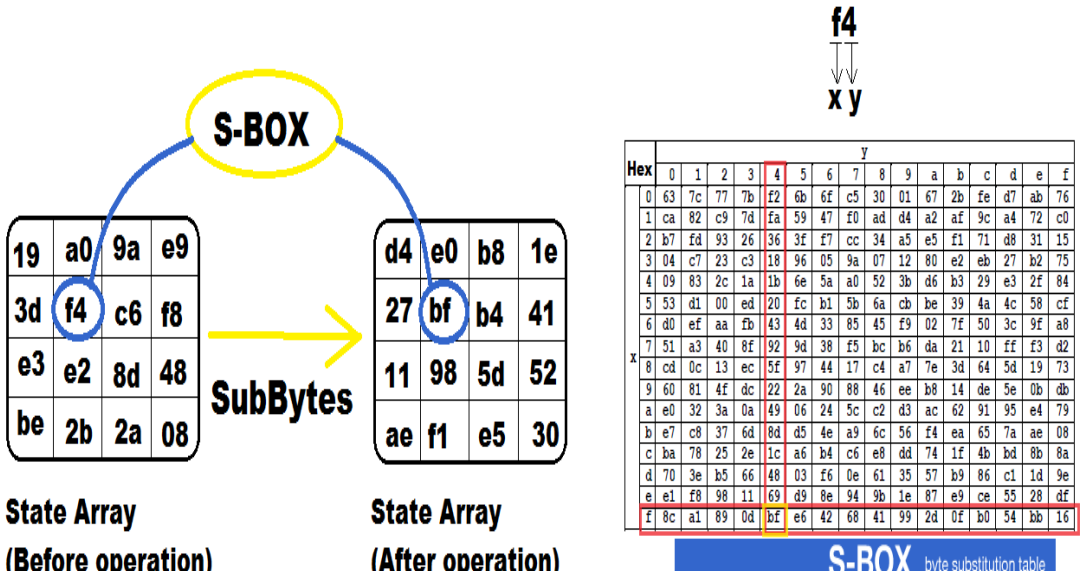


Fig. 5 Sub bytes

As shown in Fig. 5, let's take an example of "f4" data from the state array. The data "f4" is separately searched in row and column respectively and the value we get is substituted in new state array. The same operation is done for rest of the rows and columns. The final state array we get is passed on for further operations.

Shift rows: In this operation, the rows are shifted according to their respective row number. You will get a clear idea after referring the following Fig. 6.

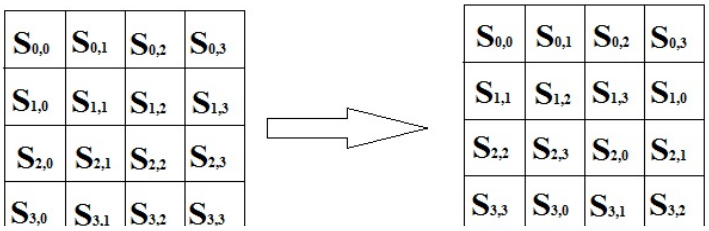


Fig. 6 Shift rows

As shown in the figure, the 0th row is not shifted whereas 1st, 2nd and 3rd are shifted by 1, 2 and 3 respectively. The final new state array is passed to later stages.

Mix columns: In this operation, each column is multiplied by a pre-defined galois matrix. Example is shown below in the Fig. 7.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

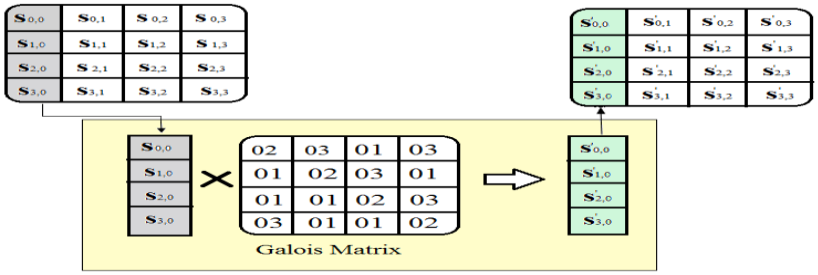


Fig. 7 Mix column

First column of state array is multiplied by galois matrix from which we get a new first column of new state array. Similarly, it is done for other columns and we get a final new state array which is passed on for further stages.

Round key generation: In this phase, a new key is generated using the previous key and the new is used for add round key operation. For each round, a new key is generated. For sake of simplicity, let's divide the operation in two phases. First phase is for getting first column of new round key. Following Fig. 8 shows an illustration of the same.

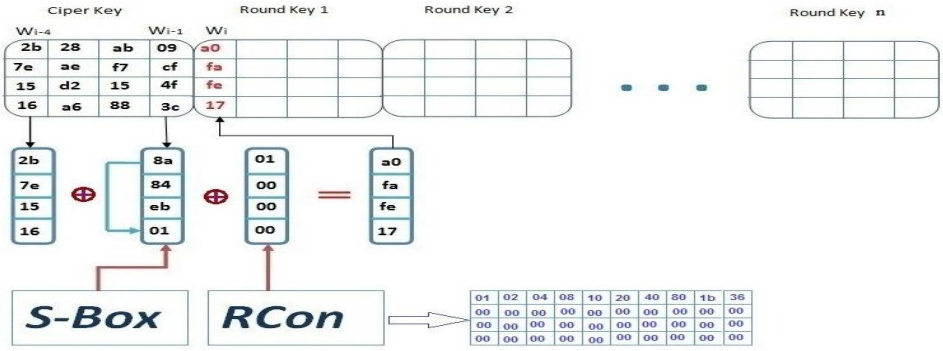


Fig. 8 Key schedule-1

As shown in the Fig. 8, the last column of previous key is taken and its top value is shifted to bottom and rest are shifted upwards.Thereafter, anrcon column is taken and first column of previous keyis taken. All the columns are XOR'ed and the resultant column is new first column of new key. For each roundkey's first column's calculation, an rcon column is taken. For first round key, first column is taken and for second round key, second column of rcon is taken and so on. Second phase is calculation of the remaining columns of new key. The Fig. 9 shows how they are calculated.

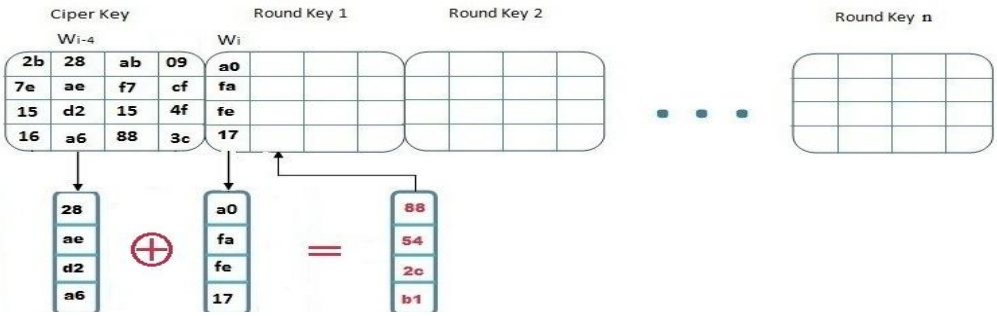


Fig. 9 Key schedule-2

As shown in the Fig. 9 for the calculation of second column, the previous column is taken i.e. W_{i-1} and W_{i-4} are taken and both are XOR'ed which gives the second column of new key and similarly, it is done for remaining two columns.The above overall process is done to get a new round key which is used for add round key operation [11].

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

IV. RESULT AND DISCUSSION

DES and 3DES presumably will take more time to encrypt because they use 64 bits of block as against of 128 bits of block of AES. DES and 3DES are said to be vulnerable against brute force attack, linear and differential cryptanalysis whereas AES is considered to be a secured algorithm with no breaks as of now is reported or published.

V. PROBLEM DEFINITION

Data should be decrypted without exchange of keys between sender and receiver and at the location specified by the sender. Additionally, there should be other parameters present like date and time to download the file in the stipulated time period and auto file destructing feature on the server after the time period is exceeded.

VI. PROPOSED SOLUTION

In this solution we would need to have two things a cloud based web services which would store the encrypted file using MySQL database at back end and a mobile application for users. For mobile applications there are many platforms available but considering the popularity of Android OS let us consider the Android application is developed. As we will be using a mobile phone for encryption, considering the computing power and battery consumption we would require we have chosen AES-128 algorithm i.e. 128 bits key will be used [8].

Firstly, a new user needs to sign up and his/her information will be stored in database on cloud service. Then after that user needs to select a contact from his list of contacts available (the receiver also needs to have the same application installedon his/her mobile phone and must have signed up then only it will be visible in sender's contact list). After selecting contact the sender needs to select the file to encrypt.

Now the user needs to specify date and time so that during that stipulated date and time the file will be visible on the receivers inbox. After the stipulated time is over the file uploaded on the server will be auto-destructed or automatically deleted. Now the sender has the option to specify One Time Password (OTP) which will be used to make the key or it will be generated automatically. The OTP is now to be sent to receiver via other channel viz SMS, email, voice call etc. whichever sender chooses according to his/her convenience. OTP can also pre-determine i.e. sender and receiver know the OTP before hand and hence there is no need of sending the OTP also which in turn increases the security. The final parameter of location is given. The location parameter is in form of the area/city name which maps the area/city to coordinates using the app built as stated earlier. Now for encryption process we have used AES algorithm (working as shown in Fig 10).

Using the date, OTP and location coordinates a 128 bit key is generated and the data is encrypted using AES. Note that time parameter is used only for making the file visible to receiver for that time only and not used for key generation. Using the generated key the file is encrypted and then sent to the server.

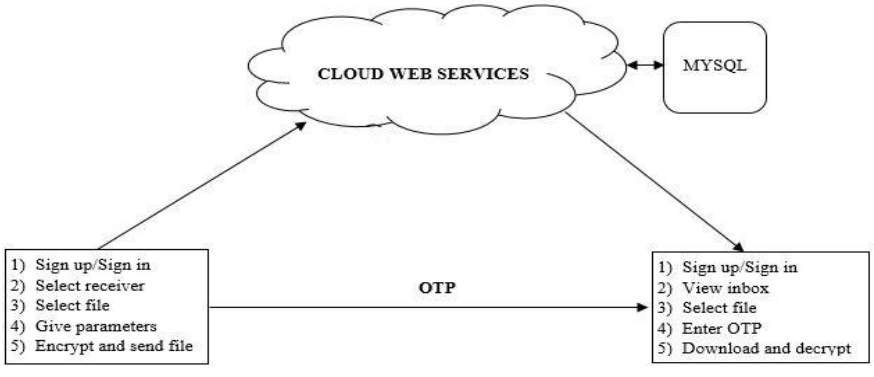


Fig. 10 Proposed Solution

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

On the receiver side, receiver will get to know that file is available to download then he/she selects the file to download and then he needs to specify the OTP and rest of the parameters required for key generation is fetched by the app itself. If he/she is at correct location then the file downloaded will be decrypted properly if not then the decrypted is not in correct form.

VII. CONCLUSION

We conclude that from above proposed solution we can improve the security of an algorithm using location and other parameters such as date and time which provides more robustness. Moreover, we don't have to exchange the keys which are needed generally in AES. Even if some else gets the file while transmitting the file that person will need the key to decrypt the file but the key is not exchanged in our solution making it stronger than usual AES. Even if the security of cloud service is compromised, and a person gets his hands on file and other parameters stored such as time and date; still that person won't have OTP which is used while making key and which is sent via other channel. Hence, he won't be able to decrypt the file.

REFERENCES

1. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key CryptographyAlgorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011, ISSN: 2250-2459.
2. Hsien-Chou Liao and Yun-Hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users", Information Technology Journal 7(1): 63-69, 2008 ISSN: 1812-5638.
3. Prasad Reddy. P.V.G.D, K.R.Sudha and P Sanyasi Naidu, "A Modified Location-Dependent Image Encryption for Mobile Information System", International Journal of Engineering Science and Technology Vol. 2(5), 2010, 1060-1065, ISSN: 0975-5462.
4. Ayesha Khan, ParulBhanarkar and PragatiPatil, " RSA Encryption Technique based on Geo Location", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013 ISSN: 2277 128X.
5. Sombir Singh, Sunil K. Maakar and Dr.Sudesh Kumar, "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 6, June 2013 ISSN: 2277 128X
6. Shah Kruti R. andBhavikaGambhava, "New Approach of Data Encryption StandardAlgorithm", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-1, March 2012, ISSN: 2231-2307.
7. Mandeep Singh Narula andSimarpreet Singh, "Implementation of Triple Data Encryption Standard using Verilog", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014, ISSN: 2277 128X.
8. Hamdan.O. Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AESwithinNine Factors", Journal of Computing, Volume 2, Issue 3, March 2010, ISSN: 2151-9617.
9. E.Thambiraja, G.Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 7, July 2012 ISSN: 2277 128X.
10. Samir El Adib and NaoufalRaissouni, "AES Encryption Algorithm Hardware Implementation: Throughput and Area Comparison of 128, 192 and 256-bits key", International Journal of Reconfigurable and Embedded Systems, Volume 1, No. 2, July,2012, pp. 67-74, ISSN:2089-4864.
11. Mr.Shelke R.B., Mrs.Patil A.P. and Dr. (Mrs.) Patil S.B., "VLSI Based Implementation of Single Round AES Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) ISSN: 2278-2834, ISBN: 2278-8735.

BIOGRAPHY

Aniruddha S. Rautpursuing Bachelor's degree from A.I.S.S.M.S. College of Engineering, Pune, Savitribai Phule Pune University, Maharashtra, India.

Harshraj N. Shindepursuing Bachelor's degree from A.I.S.S.M.S. College of Engineering, Pune, Savitribai Phule Pune University, Maharashtra, India.

Shubham R. Vidhalepursuing Bachelor's degree from A.I.S.S.M.S. College of Engineering, Pune, Savitribai Phule Pune University, Maharashtra, India.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Rohit V. Sawant pursuing Bachelor's degree from A.I.S.S.M.S. College of Engineering, Pune, Savitribai Phule Pune University, Maharashtra, India.

Vijay A. Kotkaris working as Assistant Professor in Computer Engineering Department at A.I.S.S.M.S. COE, Pune, India. He has 05 years' experience in teaching profession. He has completed his Bachelor's Degree in 2009 from A.I.S.S.M.S. COE, Pune, Pune University and obtained Master's Degree in 2013 from S.S.B.T. COET, Jalgaon, North Maharashtra University. Total 11 papers have been published and presented in various National and International Conferences and International Journals. 01 Book is published in LAP Lambert Publication, Germany. His research interest is in the areas of Image processing and Pattern recognition.