ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

ANALYSIS OF ENCRYPTION ALGORITHMS IN MOBILE CLOUD

P.Karpagam [1], K.Kuppusamy[2]

[1]Research Scholar, [2]Professor
Department of Computer Science and Engineering, Alagappa University,
Karaikudi-600 003, Tamilnadu, India.
[1]karpagam.pugal@gmail.com,[2]kkdiksamy@yahoo.com

Abstract: **In present days, mobile cloud storage is a very popular area for easy access, fast retrievable and bulk of storage files. Using this, physical data can be retrieved and processed with mobile devices like smart phones, laptops, smart mobiles, iPods etc...This stored data should be well secured by preventing unauthorized authors to attack any data. Algorithms for security have come up with large in number. In this article, analyzing the algorithm used for security is Rivest Shamir Adleman (RSA) Algorithm, Data Encryption Standard (DES) Algorithm, and Advanced Encryption Standard (AES) Algorithm. Algorithms implement the secured, encrypted data with small size of the files. There are few limitations over the orbiting system are analyzed and a proposed methodology for well secured is exposed. The accuracy over analyzing the methods of implementation is with positive higher rate.**

***Keywords*— Mobile Cloud Storage, Security, Analysis**

I. INTRODUCTION

Mobile computing and mobile sharing is the newest trend in information technology. The present mobile computing technologies are highly improved to provide effective support for all kind of mobile and wireless devices.

The mobile computing can transmit any type of files like photographs, audio files and video files without the help of any physical link [3]. Mobile computing is designed with the various network models and infrastructures like protocols and hardware components [6].

The internal mobile computing process depends on the mobile software which performs the computing processes and calculations during the user requirement. These are fundamental needs of mobile computing and these are called as the basic requirements of mobile computing.

The data security is the important issue while transmitting information's on over the web and mobile communications. Nowadays web sharing methods are mostly improved with latest security models. These kinds of security models can transact the data's with maximum security.

II. RESEARCH APPROACH

The proposed research method is a complete analysis of security algorithms, which can offer high security for mobile computing and mobile sharing.

Mobile computing and sharing tasks should be secured to make trustable communications. For example, the online banking portals provide digital signatures, virtual keyboards and encrypted code transmission [5]. The main goal is to track the reliable method which can provide highest security for mobile computing.

Cryptography is the powerful solution to provide highest security for the data's and media files. Huge number of web portals and services utilizes the cryptographic methods to offer high security for data transactions. Cryptography method includes two aspects which are encryption and decryption. Encryption involves in converting the actual content into unreadable format. The decryption involves in converting the encrypted content into original (actual) format.

The present data transfers with cryptographic approaches are offering maximum security for our data's and ensures more reliable data transfers. If the same cryptographic approaches are followed while sharing the media files on over the mobile computing technology, then it can increase the reliability and security for our data's which are transferred and maintained through mobile computing[12].

This goal of this research approach is to perform a deep analysis of cryptographic methods and find out the effective and suitable cryptographic approach for mobile sharing and mobile computing.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

III. RESEARCH METHODOLOGY

At first, the following algorithms are identified as topmost algorithms which are used in wide range of web portals.

1. RSA Algorithm
2. DES Algorithm
3. AES Algorithms

1. RSA Algorithm (Rivest Shamir Adleman):

In RSA algorithm is encrypt and decrypt data for mobile devices and modern computers. This algorithm is used asymmetric key. The implication of asymmetric key is two contrasting keys. One is public key. Public key is used for encrypt the data in cloud service providers. Another key is private key. It is an secret key. Secret key is known about user only. Private key is used to decrypt the data in original (plain text) format.

Three steps in RSA:

a. Early one is generating key
b. Plain text into cipher text (Encryption)
c. Cipher text into plain text (Decryption)

A. Generating A Key:

The original data is encrypted and decrypt before key generation is completed. This work is consummated by user and cloud service providers.

Key Generation Technique:

Initially take two distinct prime numbers. That is A and B. This A and B is randomly choosed. It is same bit length. This two prime numbers are enumerate A*B. Then compute the Euler's totient function. That function is denoted byØ(n). The formula for that function is Ø(n)=(A-1)*(B-1).The calculation is completed finally receive two disparate keys.

- Public key
- Private key

Private Key is unpublished secrete key. This private key is known only about user or who owned by the original text (massager).sender is used to encrypt the data in public key. This work is done by cloud service provider. Receiver (user) can decrypt the data using private key.

ii.Encryption:

iii.Decryption:

2. AES Algorithm (Advanced encryption standard):

AES (Advanced encryption standard is also known is Rijndael).AES is used for security like files. Files are secured by using file encryption method, files are using encrypted using password and all are based on the AES algorithm. Encrypted files can be easily accessed by the user, through uploading and downloading the files on the system. They are number of pros are available while using AES algorithm.AES is not easily harmed by a particular thing. This algorithm is much faster than the RSA algorithm.AES algorithm is the best choice for data protection. Because AES is the block cipher and it contain the block length of 128 bits. Different key lengths are used in AES algorithm are: 128,192 or 256 bits.

AES operation performs in 4*4 matrixes and it is known as column major order (CMO) matrix of bytes called the state. The key size is measured by the number of times transformation rounds that convert the plaintext, into the cipher text are repeated.

The number of repeated cycles is:

1.10 cycle for 128 bits keys
2.12 cycle for 192 bits keys
3. 14 cycle for 256 bits keys

For every encryption each round consists of four steps:

1. Key Expansion: In these step1, rounds keys are derived from the cipher key using Irondale's key schedule.

2. Initial Round: Add round key-each byte of the state is combined with the round key using bitwise X-OR.

3. Encryption performed in following rounds:

i. SubBytes: A non-leaner substitution step. Where each byte is replaced by the another byte according to a lookup table(S-box).

ii. ShiftRows: A transposition step, each row is shifted cyclically a certain number of times.

iii. Mix column: A mixing operation, which operates on the each column of the state and combine with the four bytes on the each column.

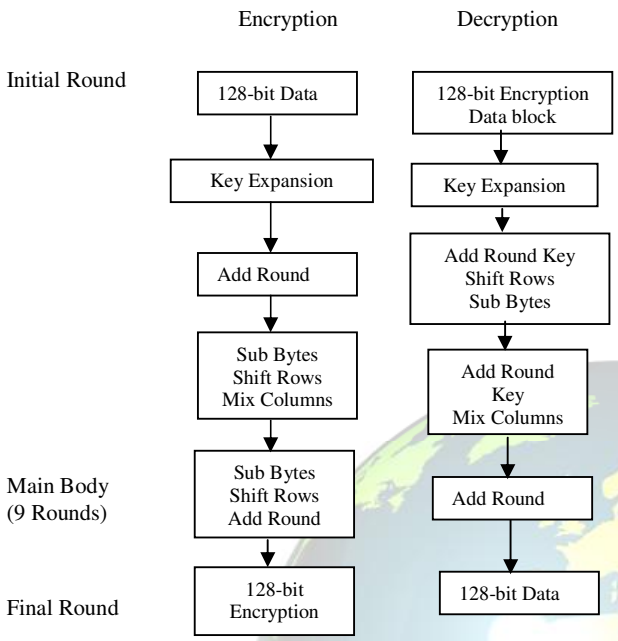
iv. Add Round key: Each byte of the state is combined with the round key, Cipherss key is derived from each round key by using key schedule.

4. Final Round (no mix columns):

1. Sub Bytes
2. Shift Rows
3. Add Round key

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Encryption and Decryption:



3. DES (Data Encryption Standard) Algorithm:

DES is a symmetric key block cipher. This cipher that performs on 64-bit blocks of data .In this algorithm, it takes a string of fixed length for plaintext and converted it into number of complicated transformations to form a cipher text bit of samelength.DES is mainly used for encrypt and decrypt the data using various transformations.

DES operates on 32 bit blocks at a time and involves four phases.

1. Expansion: In this phase by using Expansion Permutation(E) it expand the 32 bits by 48 bits. Output is based on the input, Output will contain eight pieces, and each eight pieces of length is 6 bits and it also contains a copy od 4 bit based on the corresponding input.

2. Key mixing: Using key mixing phase, the result is XOR end with the number of sub keys. Each round of the phase is retrieved from the main key using the key schedule.

3. Substitution: After the phase key mixing is finished in sub key and the block is divided into eight pieces of 6n bit length before enter them into the transformation boxes called S-boxes or substitution boxes. From lookup table substitution boxes take the input of 6 bit length and four output bis.DES security levels is maintained by a main component called S-boxes. The information should be easily hacked.

4. Permutation: Permutation is the final phase, all of the 32 output of the S-boxes are transformed to other operation based on the fixed permutation boxes is called P-boxes. After completing permutation step and output from the S-boxes are disturbed for the certain rounds.

DES Algorithm:

DES is basically designed for hardware because it is very slow in software. DES used only 56 bits. Triple DES consists three DES keys K1, K2 and K3.

1. The DES encryption algorithm:

Cipher text=EK3(DK2(EK,(plain text)))

i.e Encryption operation.DES takes K1 to encrypt the data. To decrypt DES takes K2 and again encrypt the data DES are K3.

2. Decryption is the reverse process.

Plain text = DK1(EK2(DK3(cipher text)))

i.e Decrypt with K3 encrypt with K2 and then decrypt with K1. Triple DES encrypts one block of 64 bits of data.

IV. EXPERIMENTAL RESULTS

Comparison and performance of different algorithms used in DES, AES and RSA

Parameters	DES	AES	RSA
Development	In early 1970 by IBM and Published in 1977.	Vincent Rijmen,Joan Daeman in 2001	RonRivest, Shamir& Leonard Adlemanin 1978
Key Length (Bits)	64 (56 usable)	128,192, 256	Key length depends on no. of bits in the module
Rounds	16	10,12,14	1
Block Size (Bits)	64	18	Variable block size
Attacks Found	Exclusive Key search, Linear cryptanalysis, Differential analysis	Key recovery attack, Side channel attack	Brute force attack, timing attack

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Level Of Security	Adequate security	Excellent security	Good level of security
Encryption Speed	Very slow	Faster	Average

V. CONCLUSIONS

In this proposed approach, a cryptography based mobile application is designed and coded with the above algorithms to evaluate the performance of AES, DES and RSA algorithms. The mobile application can perform the encryption and decryption with the help of Microsoft .NET framework mobile simulator. All the algorithms are tested with sample data with the help of mobile emulator and the evaluated results are tabulated above.

This study to analyse different types of encryption in mobile cloud computing. Each algorithm has individual features and methods or rules to encrypt and decrypt the data. The encryption depends upon the length of keys etc., Key has lot of bits. So that the encryption time is much more. Blowfish algorithm is very fast to work out the encryption of data compared with other algorithms such that RSA Algorithm(Rivest Shamir Adleman),DES(Data Encryption Standard) and AES(Advanced Encryption Standard).DES algorithm is the traditional encryption algorithm published in 1977.RSA algorithm is only used by asymmetric (public key) cryptosystem. Other three algorithms are symmetric key cryptosystem.DES and AES algorithms are same block size (Bits). RSA is the less secured algorithm compared with other three algorithms. AES algorithm is excellent security in encrypted data. Then next securable algorithm is Blowfish algorithm.RSA and DES has next and next levels of security.

In future, the same algorithms should be tested for image and audio data's to find the best and suitable algorithm which offers less processing time and highest security.

REFERENCES

[1] RNewswire.org, http://www.reportlinker.com/, 2012.

[2] Preston A. Coz, "Mobile Cloud Computing: Devices, trends, issues & enabling technologies", 2012.

[3] Schneider, "Essential characteristics of Mobile Cloud Computing", Marquette University, United States, 2012.

[4] Professor Kun Yang, Dr. Shumao Ou, Professor Hai Jin, Huazhong and Professor Amiya Nayak, "Mobile Cloud Computing and Networking", Proceedings of IEEE conference, 2013.

[5] M. Rajendra Prasad, Jayadev Gyani and P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges, Journal of Information Engineering and Applications", Vol 2, No.7, 2012, Print ISSN 2224-5782, pp 7 - 15.

[6] Ronnie D. Caytiles and Sunguk Lee, "Security Considerations for Public Mobile Cloud Computing", International Journal of Advanced Science and Technology, Vol. 44, July 2012.

[7] Soeung-Kon Victor Ko, Jung- Hoon Le and Sung Woo Kim, "Mobile Cloud Computing Security Considerations", April 30, 2012.

[8] Anand Surendra Shimpi and R. Chander, "Secure Framework in Data Processing for Mobile Cloud Computing", International Journal of Computer & Communication Technology, ISSN (Print) 0975- 7449, vol. 3, Iss. 3, 2012.

[9] Jibitesh Mishra, Sanjit Kumar Dash and Sweta Dash, "Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp. 347- 356.

[10] Itani et al, "Towards secure mobile cloud: A survey", Proceedings of Analyses paper, 2012.

[11] Eugene E. Marinelli, "Hyrax: Cloud Computing on Mobile Devices", Dissertation of Thesis, Carnegie Mellon University, Pittsburgh, 2009.

[12] Xiaojun Yu and Qiaoyan Wen, "Design of Security Solution to Mobile Cloud Storage",: Knowledge Discovery and Data Mining, AISC, Springer-Verlag Berlin Heidelberg H. Tan (Ed.), 2012, pp. 255–263.

[13] Robert Lemos, "Cloud's Future Security Depends on Mobile", Proceedings of RSA Conference, February 2012.

[14] V. L. Divya, "Mobile Applications with Cloud Computing", International Journal of Scientific and Research, Vol. 2, Issue 4, April 2012, ISSN 2250-3153.