IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

“Improving Data Integrity and Compressing Transmission Mobile cloud computing using RSA”

Manu sharma[1], Mandeep kaur[2]

Dept. of Computer Science Engineering, Rayat & Bahara, Mohali, India [1]

Assistant Professor, Dept. of Computer Science Engineering Rayat & Bahara, Mohali, India [2]

Abstract: Cloud computing has become an emerging standard that brings about various technologies and computing ideas for internet. Massive storage centre are provided by the cloud which can be access easily from any corner of the world and at any time. Problems faced in modern communications are not only just related to security but also concerned with the communication speed and content size, Nowdays network demand exchange of information with more security and reduction in both the data storage and the time for data transmission.The on-demand service provision with utilization of fewer resources of client system benefits the client.This can be realised by adopting an integerated approach using Merkle Hash Tree and RSA algorithm. The proposed storage security scheme also assures data integrity and recovery of data in case of data lose or corruption by providing a recovery system .Thus, the proposed scheme aims at keeping the user data restore.The system reduces the server computation when compared with previous system.

Keywords: Cryptography, Public Key Cryptography, Rivest Shamir Adlemen (RSA), Merkle Hash Tree, Cloud computing, Third Party Auditor.

I. INTRODUCTION

Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and represented as one or more unified computing resources based on sersvice level agreements established through the negotiation between the service providers and consumers. Cloud computing is a term that involves delivering hosted services over the Internet.

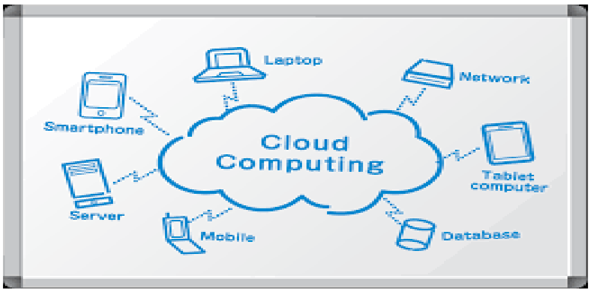

Fig1. Cloud computing Environment

By using the virtualization concept, cloud computing can also support heterogeneous resources and flexibility is achieved. Another important advantage of cloud computing is its scalability. Security in cloud means protection of information and information system from unauthorized access, modification and misuse of information or destruction. Cryptography is a technique used to avoid unauthorized access of data. Cryptography is basically divided into two categories; a) Symmetric Cryptography, and b) Asymmetric Cryptography. In symmetric cryptography the key used to encrypt the message is the same as the key decrypting the message whereas in asymmetric cryptography different key is used for encryption and decryption. Asymmetric algorithms are relatively slower than symmetric algorithms but provide a good security level. Compression/Decompression and Encryption/Decryption are encoding techniques with difference of motive one reduce the size another hide the sensitive information. Lossless compression on the other hand, manipulates each bit of data inside file to minimize the size without losing any data after decoding.The other important piece in maintaining user data in cloud is the restore system. Considering this fact, the proposed system is equipped with a recovery system which stores a backup of the user data. This contributes to availability of data anytime.

II. BACKGROUND THEORY

Client store their data at the cloud, delete the local copy of that data and rely completely on the cloud server for data safety and maintenance. For this ,auditing of the data is necessary to assure client safety of this data.

A) Client (User)
It is a network entity that stores data on the cloud server and relies on it for the maintenances and storage of the data.

B) Cloud Service Provider (CSP)
It is the cloud server that provides significant storage space,resources and maintenance for user data.

C)Third Party Auditor (TPA)
TPA is an entity that has knowledge and expertise that client does not possess. It is responsible for data integrity verification and works on behalf of the client.

D) Merkle Hash Tree (MHT)

Merkle Hash Tree is a well-studied authentication structure. It is used to efficiently prove that a set of elements are undamaged and unaltered. It helps greatly in reduction of server time . It is used by cryptographic methods to authenticate the file blocks. The leaf nodes of the MHT are the hash values of the original file blocks. The idea behind generating MHT is to break the file into a number of blocks. Apply hashes to the authentic data values i.e. the original file blocks and combine iteratively. Now, re-hash the result hash nodes and combine in a tree-like fashion and repeat this procedure till we get a tree with a single root. The MHT is generated by the client and is stored at both the client and the server side.

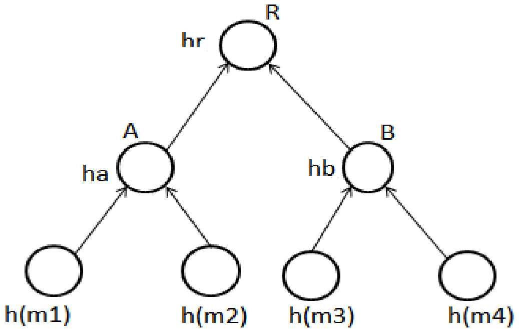

Fig.2 Merkle Hash Tree

The above constructed figure depicts an example of MHT. The tree has four leaf nodes viz. m1, m2, m3 and m4. Initially, we apply hash on each of these file blocks and obtain h(m1), h(m2), h(m3) and h(m4). Then, h(m1) and h(m2) are hashed and combined together to get ha. Similar process happens with blocks m3 and m4 and here, we get hb. Here, h is a secure hash function. This can be expressed as ha = h(h(m1)|| h(m2)) and hb = h(h(m3)|| h(m4)) Further, ha and hb are combined and rehashed to obtain the root as hr. This can be expressed as

hr= h(ha|| hb)

III. PROPOSED SCHEME

In our proposed work, RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider .Cloud provider authenticates the user and delivers the data.

System Framework and methodology

RSA algorithm **:** RSA algorithm is designed by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT in 1978 .RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public Key, it can be decrypted with the corresponding Private-Key only. Thus only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm as well and encrypted data is been autoback to hidden server.

Practical Implementation of RSA Algorithm

To implement RSA, one has to focus on three parts which are
a) Key generation
b) Encryption process
c) Decryption process

Key Generation Algorithm**:**

There are two types of keys in RSA; public key and private key. The steps for key
generation are given as:

1). Generate two large prime numbers p and q.
2). Compute n = p*q
3). Compute z= (p-1)*(q-1)
4). Choose a number relatively prime to z and call it d .
5). Find e such that e*d = 1mod z.
6). Public key is (n,e).
7) Private key is (n,d).

Encyption algorithm

It is the process of converting the original text into the cipher text data.
Following are some of the steps :
1) Obtains the recipient public key (n,e).
2) Represents the plain text message as positive integer.
3) Compute the cipher text $c = m^e \mod n$
4) Sends the cipher text.

Decryption algorithm

Decryption is the process of converting the cipher text (data) to the original plain text (data)
Following are some of the steps :
1) User request the service provider for the data
2) The service provider verifies the authenticity of the user and then gives the encrypted data i.e. C
3) The user decrypts the data by computing

$$m = c^d \mod n$$

Extracts the plain text from integer representing m .

RSA with Merkle Hash Tree algorithm

This Combination of two techniques called the RSA with Merkle Hash Tree Algorithm shown in the Block diagram shows that if workstation1 want to send the text message to workstation 2 then it inputs the text file to proposed technique and proposed technique compress the size of the text with Merkle hash tree algorithm and also encrypt the message with RSA in the form of cipher text so that intruder never understand the message and the transmission of the message can be speed up.

This combination of elements is a message, M. This message from the alphabet, A is encoded into the binary alphabet, B. The string of bits, binary digits (0's and 1's), is the encoded data in the forms of blocks of 1024 bits. So essentially encoding is just transferring a message M, from the alphabet A into the alphabet B.

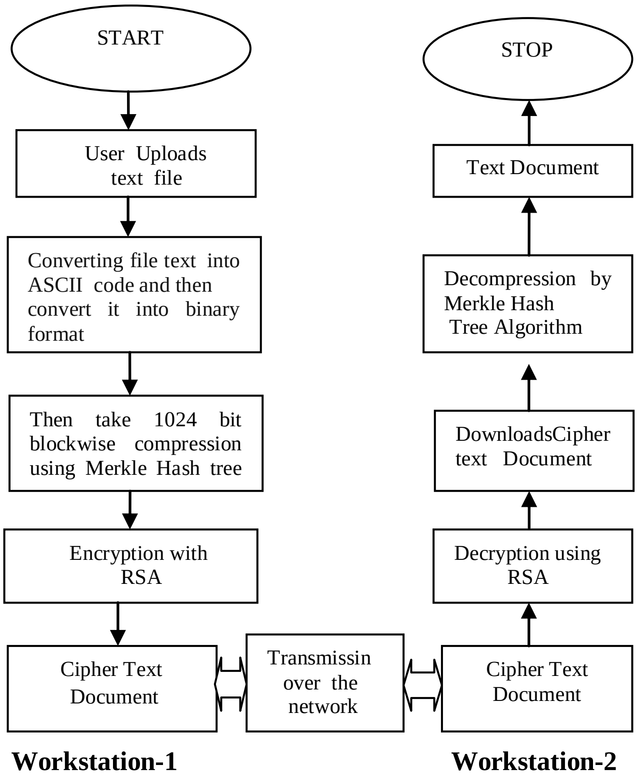
START
User Uploads text file
Converting file text into ASCII code and then convert it into binary format
Then take 1024 bit blockwise compression using Merkle Hash tree
Encryption with RSA
Cipher Text Document
Transmissin over the network
Cipher Text Document
Decryption using RSA
DownloadsCipher text Document
Decompression by Merkle Hash Tree Algorithm
Text Document
STOP
Workstation-1
Workstation-2

Fig.3 Block diagram of combining RSA and Merkle Hash Tree Algorithn

Algorithm Design

1) Firstly the user will login Click on the login.
You will be then prompted to enter your username and password. If you have not logged in before, you will need to register yourself by providing details such as name, fathers name , email address and password etc to create an account and use cloud services.

2). Then upload the data on the cloud servers.
Uploading is the transmission of a file from one computer system to another, usually larger computer system or mobiles. To upload a file in a cloud is to send file to another computer that is set up to receive it. To upload new data to cloud. Click on upload button it will display the Data set . Select the file you want to upload .

3) Encryption of the data will be done
The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text encrypted data is referred to as cipher text.

4) The uploaded data will get stored in File server1 and File server 2.

5) When user download the data then the uploaded data will decrypt and comes in original form.

IV. RESULTS

The five text files of different sizes are used to conduct experiments, where a comparison of three algorithms AES, DES and RSA is performed. A cryptography too is use to conduct experiments.

Performance of encryption algorithm is evaluated considering the computation time. The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text.Encryption time is used to calculate the throughput of an encryption scheme.

Encryption Computation Time

The encryption computation time is the time which is taken by the algorithms to produce the cipher text from the plain text.

Graphical representation of time taken for encrypting files of different sizes by AES , DES , RSA & RSA* (Proposed RSA) algorithms.

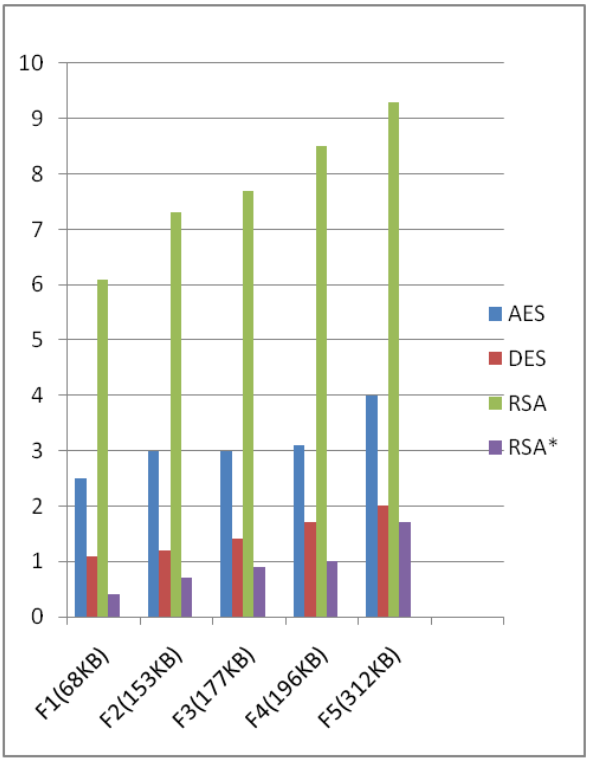

Fig.4 Comparison analysis of Encryption

Decryption Computation Time

The decryption computation time is the time which is taken by the algorithms to produce the plain text from the cipher text.

Graphical representation of time taken for decrypting file of different sizes by AES , DES ,RSA & RSA*(Proposed RSA) algorithms.

Outcome:

It has been observed that proposed approach provides better throughput for all types of file sizes when compared to other algorithms. Results prove that the proposed algorithm is optimized compared to other algorithms in terms of hacking and processing time.

DOI 10.17148/IJARCCE.2016.53174

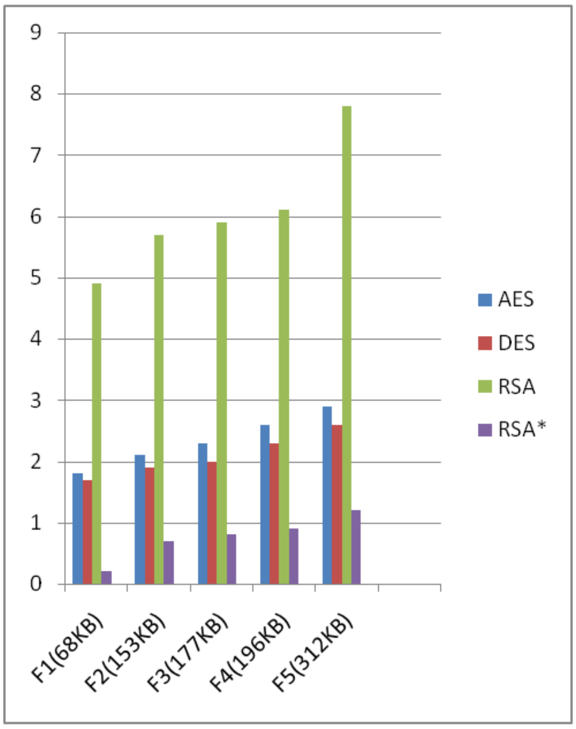

Fig.5 Comparison analysis of decryption timings

V. CONCLUSION AND FUTURE SCOPE

The aim of the cryptography is to prevent data from hackers. Study of various encryption algorithms has been successfully done. It has been shown that the time taken by the algorithm to encrypt or decrypt files depends on the size of file. Size of file is inversely proportional to time . As the file size is increased performance degrades .After critically analyzing RSA; it is found that there are flaws in it and so to overcome these flaws a new algorithm has been proposed. The proposed algorithm increases the security of the system and also reduces the computation time; therefore hacking time is reduced which indicate that the time available for the hacker has been reduced. The proposed algorithm has been compared with other algorithms, and it is found that throughput of proposed algorithm is greater than other encryption algorithms.The RSA at last level gave this research a brilliant security that this architecture is fully secured for any kind of confidential data preservation along with good results than previous basic AES and DES algorithms. The work can be extended to decrease the complexity of proposed algorithm.

ACKNOWLEDGEMENT

First of all I want to thank the light of god who guided me throughout the way. Then apart from the efforts from me, I would like to show my greatest appreciation to my guide **Mrs.Mandeep Kaur**,(Assistant Professor) for her great efforts of supervising and leading me to accomplish this fine work.

REFERENCES

[1] A. J. Elbirt, W. Yip, B. Chetwynd and C. Paar, “An FPGA Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists”, IEEE Transactions on Very Large Scale Integration Systems, Vol. 9, No. 4, pp. 545-557,2001.

[2] A. Khalique, K. Singh and S. Sood, “ A Password-Authenticated Key Agreement Scheme Based on ECC Using Smart Cards”, International Journal of Computer Applications, Vol. 2, No.3, pp. 26-30, 2010.

[3] A. Kakkar and P. K. Bansal, “Reliable Encryption Algorithm used for Communication”, M. E. Thesis, Thapar University, 2004.

[4] Bharat B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan and K.S. Trivedi, “Method for Modeling and Quantifying the Security Attributes of Intrusion TolerantSystems”, Journal of Performance Evaluation, Elsevier Science Publishers, Vol. 56,No. 1, pp. 167-186, 2004.

[5] C. H. Kim, “Improved Differential Fault Analysis on AES Key Schedule”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 41-50, 2012.

[6] C. P. Su, T. F. Lin, C. T. Huang and C. W. Wu, “A High-Throughput Low Cost AES Processor”, IEEE Communications Magazine, Vol. 41, No. 12, pp. 86-91, 2003.

[7] E. Bertino, N. Shang and S. S. Wagstaff, “An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting”, IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 2, pp. 65-70, 2008.

[8] F. Menichelli, R. Menicocci, M. Olivieri and Alessandro Trifiletti, “High Level Side Channel Modeling and Simulation for Security Critical Systems on Chips”, IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp. 164-175,2008.

[9] Garg, P.; Sharma V., "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function," in Issues and Challenges in Intelligent Computing Techniques (ICICT)”, 2014 International Conference on , vol., no., pp.334-339, 7-8 Feb. 2014

[10] H. C. Williams, “A Modification of the RSA Public-Key Encryption Procedure”,IEEE Transactions on Information Theory, Vol. 26, No. 6, pp. 726-729, 1980.

[11] Hua Li and J. Li, “A New Compact Dual-Core Architecture for AES Encryption and Decryption”, IEEE Canadian Journal of Electrical and Computer Engineering, Vol.33, No. 3, pp. 209-213, 2008.

[12] H. Chien, “Efficient Time-Bound Hierarchical Key Assignment Scheme”, IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 10, pp. 1301-1304, 2004.

[13] H. W. Kim and S. Lee, “Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System”, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 214-224, 2004

BIOGRAPHIES

Manu Sharma is Pursuing Masters of technology in Computer Science Engineering from Rayat & Bahara College Mohali, Punjab (India).She received the degree of Bachelor of Technology in Computer Science Engineering from Rayat & Bahara College Mohali, Punjab (India).Her area of interest is Network security issues faced by the users in the computer networks and RDBMS.

Mandeep Kaur received her M.Tech degree in Computer Engineering. She has more than 5 years of teaching experience. Presently she is working as Assistant Professor in Rayat Bahara Collage of Engineering & Biotechnology, Mohali, Punjab.

DOI 10.17148/IJARCCE.2016.53174