RESEARCH ARTICLE OPEN ACCESS

Multilevel Security for Data as a Service (Spacebox) Using Cryptography

Prof. Sachin H. Darekar, Sayali Zende, Prerana Pawar, Akanksha Pinglaskar
Bharati Vidyapeeth College of Engineering
Sector-7, C.B.D, Belpada, Navi Mumbai-400614, India.

----------**********----------

Abstract:

There Abstract- cryptanalyst are professional in how to fracture the encryption techniques. We require securing our programs and documents from cryptanalyst. Security of information means protecting data from unauthorized right to use in cloud environment. There are many techniques to reach the security of information from unauthorized entrance. There are two cryptographic techniques used for data encryption which are symmetric and Asymmetric techniques. Symmetric key encryption algorithms are computationally fast compared to asymmetric encryption algorithms (Like RSA). However, since the identical secret key is used for symmetric encryption and decryption, we have the crisis of securely distributing that secret key. Asymmetric key infrastructure in PKI does not rely on circulation of any private key. However, the familiar asymmetric algorithms are used for bulk encryption with recent computation capability. While SHA is collision resistant to a variety of block cipher algorithms. Thus for superior security performance, we propose a system which would integrate the advantages of these algorithms namely SHA, RSA which will be a hybrid approach of encrypting data. SHA is adopted in this mechanism to verify the integrity of the significance. Three major security principle such as authentication, confidentiality and integrity are achieved together using this method.

----------**********----------

I. INTRODUCTION

In today's times Cloud computing has a significant impact on the IT industry. With growing popularity more and more organizations are making use of cloud services. Although Cloud services have a dispread acceptance but the fear pertaining to security and privacy of these services continue to be an open challenge. With rapid technological advancements these services could be accessed through smart phones thus allowing users to share pictures, video, documents and other important data across various platforms on a real time basis. However, a security breach in their security has always been a concern in the domain of information technology. With Cloud services handling critical data which can be accessed from anywhere though the internet makes security a prominent concern. While talking of Cloud security there are many aspects which one needs to consider such as, trusted authentication, appropriate authorization data security and privacy. Data encryption has been one of its key measures in ensuring data security protection.

It is a method of encrypting the original information into a form that is not interpreted by anyone. Original message can be revealed only after decrypting the encrypted message. Public and private

keys are used for this purpose. Generally, the cryptographic systems can be classified into symmetric and asymmetric. In symmetric cryptography, same key is used for the encryption and decryption whereas

- Symmetric key cryptography algorithm

To raise the security level, this proposed scheme overcomes the restriction of "Basic encryption algorithm planned till date. The proposed enhanced method includes RIJNDAEL, RSA and SHA. RIJNDAEL strengthens the security of data stored in cloud. Cause behind for selecting RIJNDAEL rather other encryption algorithms is that, the key used for encryption and decryption is suspected to meet-in-middle attack. RSA is used to solve the key distribution crisis and in count to this, SHA to authenticate the integrity of the data. Use of SHA algorithm in combination of cryptographic algorithm provides strength in security of data stored in cloud.

II. LITERATURE SURVEY

Sr no.	Name of paper	Technology used	Advantages	Disadvantages
1.	Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing Author: Long wang,kui Ren	KeyGen, SigGen, Genproof, Verify proof Algorithm's.	1. Data outsourcing is done efficiently. 2. System eliminates the burden of cloud users.	External parties auditing during the process so, this system cannot completely solved the problem of protecting data privacy.
2.	Implementation Vulnerability Associated with OAuth 2.0 (A Case Study on DropBox) Author: Mohammad Husain	OAuth 2.0 (protocol),security token	OAuth provide the client access behalf the resource owner, without sharing resource owner credential.	This system provide the token, but the time of token created while registration in not implemented in the variable.

in asymmetric cryptography separate keys are used for the encryption and decryption process. There are two types of cryptography algorithms that are given below:

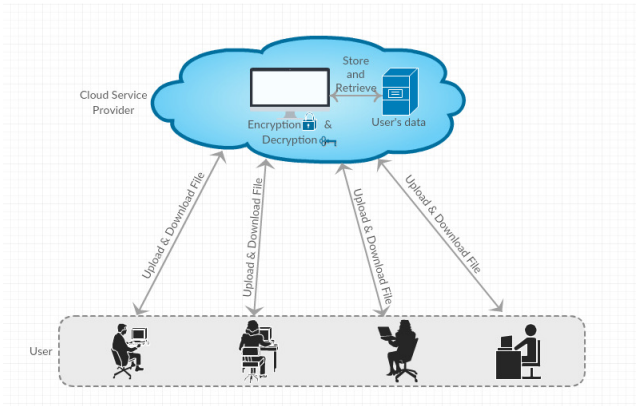
- Asymmetric key cryptography algorithm

III. SYSTEM ARCHITECTURE

The front end system gives graphical user interface (GUI) in the form of a browser expansion using Visual Studio 2013. The clients interact with the organization where backend includes storing user's data in an encrypted form. The encrypted information like pdf, doc, and text file are stored in SQL Server 2014 database. When the user uploads new file other user is allow to see name of new file. If other user wants the access that file then he can send access request for the particular file. The file owner gets notice of the file requested and if he/she responses appeal then requested user can get right of entry to that file.

IV. PROPOSED SYSTEM

In this paper, we proposed a hybrid encryption technique is useful on the data file using AES, RSA and SHA algorithm to securely store data file in cloud. This system application will form and create opportunities that offer users to keep their data files on cloud storage in an encrypted form.



AES algorithm

The Advanced Encryption Standard (AES) is a symmetric key block cipher algorithm. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is limitless, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not affect the Data Encryption Standard (DES) network.

1. Key Expansions-round keys are derived from the cipher key using AES key schedule. AES require a separate 128-bit round key block for each round plus one more.
2. Initial Round:
   a. Add Round Key-each byte of the state is combined with a block of the round key using bitwise XOR.
3. Rounds:

a. Sub Bytes-a non-linear substitution tread where each byte is replaced with a new according to a lookup table.

b. Shift Rows-a transposition tread where the last three rows of the status are shifted regularly a certain number of steps.

c. Mix Columns-a mixing operation which operates on the columns of the state, combining the four bytes in each column.

d. Add Round Key.

4. Final Round (no Mix Columns):

a. Sub Bytes

b. Shift Rows

c. Add Round key.

SHA

Secure Hash Algorithm (SHA)-512 is an alternative of SHA-256 which operates on eight 64-bit words. The message to be hashed is first

(1) Padded with its length in such a way that the result is a multiple of 1024 bits long, and then

(2) Parsed into 1024-bit message blocks.

The message blocks are processed one at a time: Beginning with a fixed initial hash value. The SHA-512 solidity function operates on a 1024-bit message block and a 512-bit intermediate hash value. It is essentially a 512-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Hence there are two main mechanisms to describe:

A. the SHA-512 solidity function, and

B. the SHA-512 message schedule.

RSA algorithm

1. Rivest-Shamir-Adleman (RSA) keys are typically 1024- or 2048-bits long, but experts believe that 1024-bit keys could be broken in the near future, which is why government and industry are moving to a minimum key length of 2048-bits.

2. In RSA cryptography, equally the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This aspect is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

3. RSA derives its security from the complexity of factoring large integers that are the invention of two outsized prime numbers. Multiplying these two numbers is effortless, but determining the original prime numbers from the totality -- factoring -- is considered infeasible due to the time it would take even using today's super computers.

V. CONCLUSION

In this system hybrid encryption technique is applied on the data file using AES,RSA and SHA algorithm to securely store file data in cloud.This system purpose will structure and build opportunities that tender users to keep their data files on cloud storage in an encrypted form. The user will share his files with the recognized person so system eliminates the burden of cloud users regarding the security and share files efficiently but the shared data will be in the form of link. User can click on link and download the shared file.

VI. REFERANCE

[1] 2016 IEEE International Conference on Cloud Computing in Emerging Markets 'Securing Files in the Cloud'.

[2] Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing matter experts for publication in the IEEE INFOCOM 2010

[3] Implementation Vulnerability Associated with OAuth 2.0 a case study on DropBox 2015 12th International conference on information Techonolgy-newGeneration.

[4] SQL Server 2014: https://www.youtube.com/results?search_query=sql+server2014

[5] ASP.net: https://www.youtube.com/results?search_query=ASP.net+2013

[6] Cloud computing: https://www.youtube.com/watch?v=QJncFirhjPg

[7] www.google.com

[8] En.wikipedia.org