ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Non Repudiation Protocol in Network Security

Shraddha G. Kokate[1]
Computer Science and Engineering
H.V.P.M's C.O.E.T
Amravati, India

Ranjit R. Keole[2]
Professor
Information Technology
H.V.P.M's C.O.E.T
Amravati, India

Abstract: ***This document gives formatting instructions for authors preparing papers for publication in the Proceedings of an International Journal of Advance Research in Computer Science and Management Studies. The authors must follow the instructions given in the document for the papers to be published. You can use this document as both an instruction set and as a template into which you can type your own text.***

Keywords: component; authentication,; confidentially; integrity; RSA

I. INTRODUCTION

The Non repudiation protocol in cloud networking is a large-amount of distributed computing paradigm driven at economics scale, in which a pool of abstracted, virtualized, dynamically-scalable, highly available and configurable and reconfigurable computing resources can be rapidly provisioned and released with minimal effort in the data centers. Another typical situation parallels a common human need: in order to transfer funds from one person to another. In other words, we want to be able to send electronically the equivalent of a computerized check. We understand how this transaction is handled in the conventional, paper mode. The Non Repudiation Protocol is a protocol that produces a same effect as a real signature. It is a mark that only the sender can make, but other people can easily recognize as belonging to the sender. Just like a real signature, Non repudiation protocol is used to confirm agreement to a message

II. EASE OF USE

a) Public-Key Cryptography

In cryptography, secret writing is the strongest tool for controlling against many kinds of security threats.It is not necessary to understand the underlying mathematics to be able to use cryptography. When most people who are not versed in cryptographic concepts think of encryption, they generally think of symmetric cryptography. That is, cryptography where you encrypt a message using a secret key, and use that exact same key to decrypt the message. all the schemes discussed in this paper will concern asymmetric cryptography, better known as public-key cryptography.

The basic idea behind public-key cryptography is as follows: Rather than having one key to encrypt messages, each user has two related keys that is a pair of keys are used. The sender uses the public key and receiver uses the private key. Tnhe other is the private key or symmetric key cipher, the same key is used by both the sender and receiver. The key is called secret key. that is used to decrypt messages that were encrypted using the public key. Alice, wishing to send Bob a message, must look up his public encryption key and encrypt her message using it. Once she has encrypted the message, neither she nor anyone else (including Bob) can decrypt it using the public encryption key. Bob, using his private key that only he should know can easily retrieve the original message from the ciphertext sent to him. These algorithms are based on one-way functions, which we will now discuss.

b) General Description of Symmetric (Private-Key) Cryptography

k is the key agreed on beforehand by Alice and Bob, m is the message to be sent from Alice to Bob,

k E is the encryption algorithm using key k,

k D is the decryption algorithm using key k

Alice encrypts message M using E (m) k and sends it to Bob.

Bob decrypts using D (E (m)) k k and recovers the message M.

c) General Description of Asymmetric (Public-Key) Cryptography

m is the message to be sent from Alice to Bob,

B E is the encryption algorithm using Bob's public key,

B D is the decryption algorithm using Bob's private key.

Alice encrypts the message m using E (m) B and transmits the results to Bob

Bob decrypts using D (E (m)) B B and recovers the message m..

III. ENCRYPTION ALGORITHM

A private Key cryptography uses one key. Key is shared by both sender and receiver. If the key is disclosed communications are compromised, also known as symmetric, both parties are equal .Hence does not protect sender from receiver forget a message & claiming is sent by sender. developed to address two key issues.

Key distribution- To secure communications in general without having to trust a key distribution cryptography (KDC) with your key.

Digital signatures- how to verify a message comes intact from the claimed sender. The code of the security model shown as following diagram

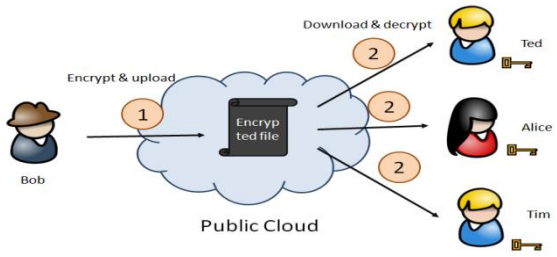

Fig 1 proposed cloud network

Figure 1 is the pictorial representation of the proposed cloud network. Here, single user and server represent multiple user and multiple servers. The algorithm says, which is used add the file in the main system (Server). Where encrypted file kept in database table soaked from the server system for the cloud computing environment. Inserted data's maintaining sequence order. The system server table and database server tables can be through as disjoint sets.

IV. CRYPTOGRAPHY ALGORITHM

The Cryptography algorithm are classified as following

1. RSA

2. AES

3. SHA.

a) RSA(Rivest, Shamir &Adleman of MIT in 1977)

The RSA algorithm cryptosystem is a public key sytem. The RSA encryption algorithm incorporates result from number theory, combined with the difficult of determining the prime factors of target. The RSA algorithm also operates with arithmetic mod n. Three approaches to attacking RSA:

» Brute force key search (infeasible given size of numbers)

» Mathematical attacks (based on difficulty of computing ø(N), by factoring modulus N)

» Timing attacks (on running of decryption).

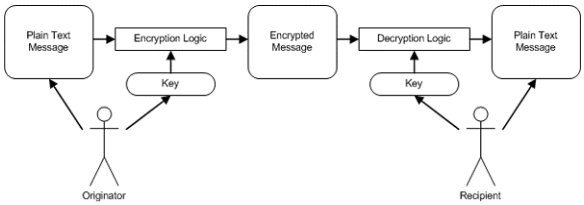

Fig 2 Encryption in RSA Algorithm

The RSA algorithm sender and receiver send a hypertext to plaintext. It converts ASCII value.

Algorithm:

1. p&q where p&q are prime numbers.

2. n=p&q.

3. Congruence modules ϴ(x)=(p-1)*(q-1).

4. Public key e is given =2.

5. Tfind out the private key d*e mod x=1.

6. Encryption: c=m€ mod ϴ (x).

Decryption: m=c(d) mod ϴ (x).

b) AES (ADVANCED ENCRYPTION STANDARD)

AES is round cipher based on the Rijndael algorithm that uses a 128 bit blocks of data. AES has three different configurations: 10 rounds with a key size of 128 bits, 12 rounds with a key size of 192 bits and 14 rounds with a key size of 256 bits. In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data. The Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Festal network.

The main loop AES performs the following functions:

1. sub Bytes(Scramble each byte).
2. Shift Rows(subByte).
3. Mix columns(Scramble each column).
4. AddRoundkey(AddRoundKey).

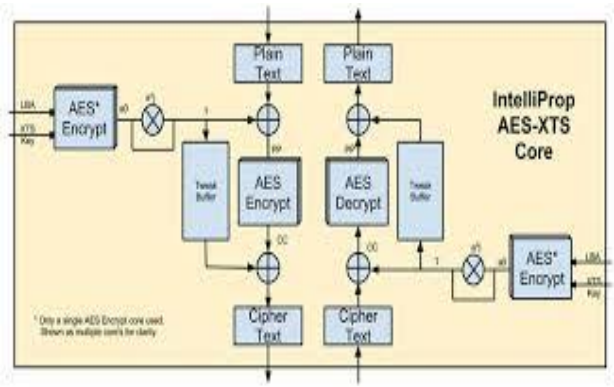

Figure 3 Encryption in AES

c) SHA(Secure Hash Algorithm)

There are quite a number of cryptographic hash functions that is created by the National Institute of Standards and Technology. One of these functions is the Secure Hash Algorithm(SHA),which corresponds to the Federal Information Processing Standard of the United States of America. SHA encryption is a series of five various cryptographic functions and this presently has three generations: SHA-1, SHA-2, and SHA-3. The first SHA generation is SHA-1 and it is the fundamental 160-bit hash function. SHA-1 appears similar to the former algorithm MD5. The organization responsible for the establishment of this function is the National Security Agency (NSA) and it has a primary role as a branch of the Digital Signature Algorithm. SHA-1 was commonly used in security protocols like the PGP, TLS, SSH, and SSL.

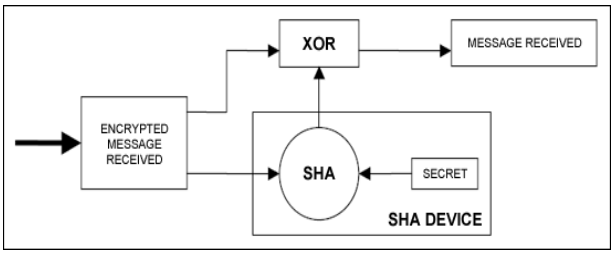

Figure 4 Secure Hash Function

V. PROPOSED MODEL

A proposed security model in a cloud networking ,here file one encrypted with RSA algorithm in which the keys are created sequentially one by one to the system. This ensuring a major secures and also solve the main security issues like a new login user data hacking to the attacker. Login into the main system is compulsory and download, store the files. The encrypted file is hide from intruder. In this files already store the main system server. It only single user multiple servers. The user forgets a password and not able to use same user name have key value to identify unique values. Once login the entry detail is cannot access the same user name login.

ACKNOWLEDGMENT

My thanks to the Guide, Prof. R.R.Keole and Principal Dr.A.B.Marathe, who provided me constructive and positive feedback during the preparation of this paper.

References

1. Yashapalkadam,:Security in cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology,Vol-2 N October,2011,316-322.
2. Shobha Rajak, Ashok Verma "Secure Data Storage in the Cloud using Digital Signature Mechanism" IJARCET June 2012
3. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 Prepared by Cloud Security Alliance December 2009
4. Defining Cloud Deployment Models, http://bizcloudnetwork. Com/defining-cloud-deployment -models

5. Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.

6. Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference

AUTHOR(S) PROFILE

Shraddha G. Kokate received the B.E.degree in Computer Science and Engineering from Shree Shivaji College Of Engineering And Technology, Akola in 2011. She is currently persuing Master's Degree in Computer Science and Engineering from H.V.P.M's College of Engineering And Technology, Amravati.

Prof. Ranjit R.Keole, received the B.E.and M.E degree in Computer Science from Prof. Ram Megha Institute of Technology, Badnera in 1992 and 2008, respectively. His field of specialisation is web Mining. He is currently working as Associate Professor at H.V.P.M's college of Engineering and Technology,Amravati.

