ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing

T. Sivasakthi[1] and Dr. N Prabakaran[2]

Research Scholar, Department of Computer Applications, St.Peter's University, Avadi, Chennai – 600 054, India[1]

Associate Professor, Department of Computer Applications, Rajalakshmi Engineering College, Thandalam Chennai – 602 105, India[2]

ABSTRACT: The cloud computing is Internet based computer, shared software information and resource to world. These cloud environment resources are shared to all servers, and separate users. The cloud computing supports distributed services multi-domain Infrastructure, and multi-users. This paper proposed user authentication to secure data of encryption algorithm with digital signature in cloud computing. This infrastructure guaranteed to secure the information in cloud server.

.

KEYWORDS: Cloud computing, security, AES, RSA, Digital signatures.

I.INTRODUCTION

The technology of distributed data processing in which some scalable information resources and capacities are provided as a service, to multiple external customers through Internet technology. The concept of cloud computing there are also common notion Data as a service and everything as a service respectively. Both concepts show that, through the World Wide Web using Cloud Computing can meet any requirements in the processing of information. This is the main advantage of cloud computing in the IT-based business solutions.

- Cloud computing is an umbrella term used to refer to Internet based development and services
- A number of characteristics define cloud data, applications services and infrastructure:
  - ***Remotely hosted*** - Services or data are hosted on remote infrastructure.
  - ***Ubiquitous*** - Services or data are available from anywhere.
  - ***Commoditised*** - The result is a utility computing model similar to traditional that of traditional utilities, like gas and electricity - you pay for what you would want.

II. ENCRYPTION ALGORITHM

Public invention due to Whitfield Differ & Martin Hellman at Stanford U. in 1976Traditional private/secret/single 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

- 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.

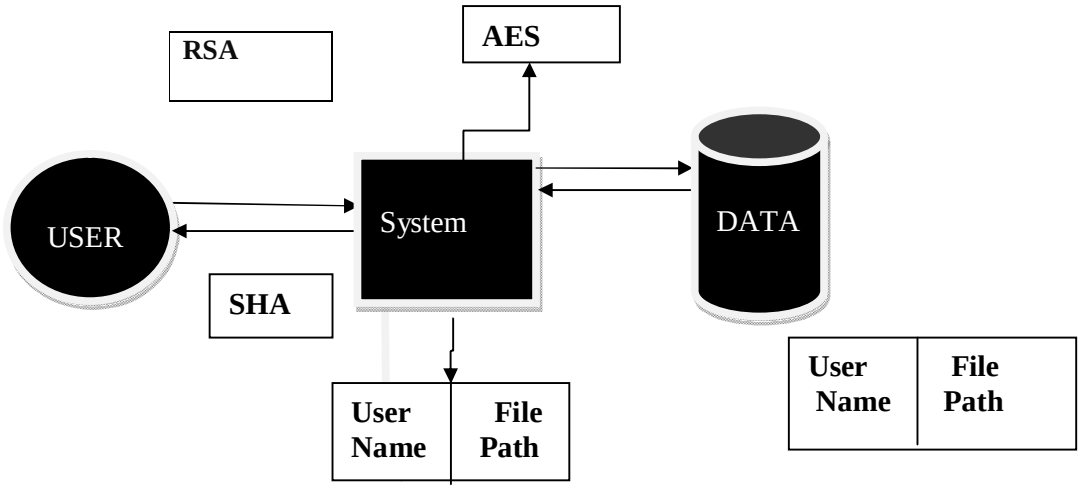

Figure 1: Proposed Security Model/Structure

Figure 1 is the pictorial representation of the proposed security architecture. 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.

III. CRYPTOGRAPHY ALGORITHM

The Cryptography algorithm are classified as following

1. RSA
2. AES
3. SHA.

1. *RSA(Rivest, Shamir &Adleman of MIT in 1977)*

Best known & widely used public-key scheme based on exponentiation in a finite (Galois) field over integers modulo a prime nbexponentiation takes O $((\log n)^3)$ operations (easy) uses large integers (eg. 1024 bits) security due to cost of factoring large numbers .nb.Factorization takes O($e^{\log n \log\log n}$) operations (hard) .

- 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).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

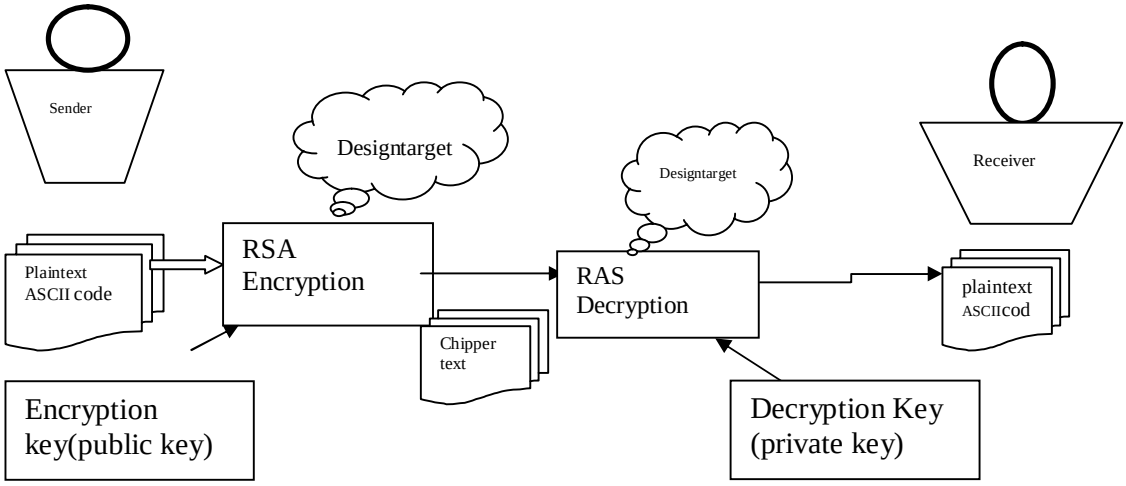

Figure 2: RSA algorithm work flow diagram

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).

2. AES (ADVANCED ENCRYPTION STANDARD)

The AES is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. 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 AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. 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).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

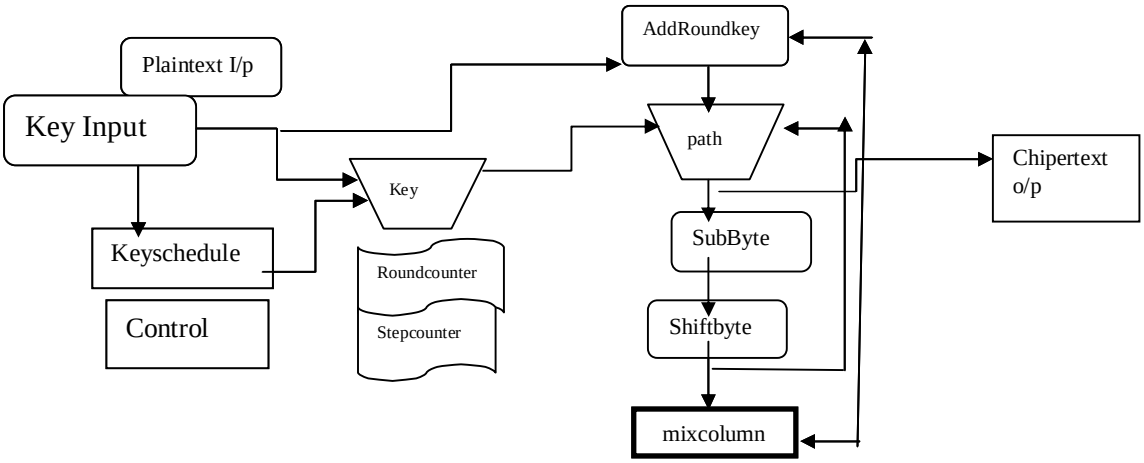

Figure 3: AES algorithm work flow diagram

3.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.

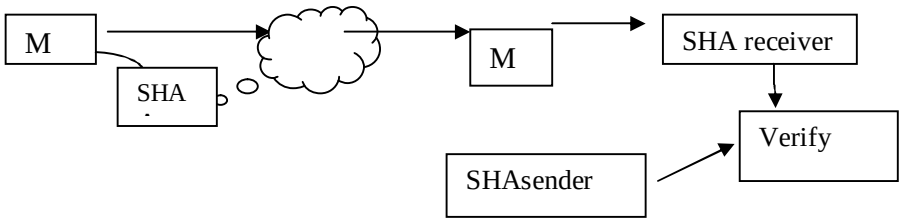

Figure 4: SHA algorithm work flow diagram

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Related work:

Sno	Citation	Paper Name	According this paper
1.	Yashpalkadam	Security issues in cloud computing**.**	Persons interconnected with network environment, recently major challenges in cloud computing.
2.	Ranjitemishra	A privacy presenting repository for securing Data across the cloud.	The facilitate data showing and integrating along with data conformations. This has been encrypting technique to data storage**.**
3.	QianlishenTong,Jiyiwu.	Recent advance in cloud security**.**	Its mainly providing security for a file and its present are user secured channel for communication**.**
4.	Anujgupta	Secure Data storage and ret rival in the cloud.	The communicated between user and server is, not encrypt the loaded information. This ensures the uploaded information and encrypts the data location easily to secure the information.
5.	KawerwazedNafi,tonnyshekha,kar.	New user authentication distributed server based cloud computing security architecture**.**	Unauthorized user login the system only one time enter the details for main account. Advantages by making use of multiple distinct cloud data at the sequence of time.

IV.PROPOSED MODEL

A proposed security model in a cloud computing environment,here file one encrypted with RSA algorithm in which keys are created sequence one by one to the system. This ensuring a major secures and also solves 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 a file is hide from unauthorized users. In this files already store the main system server. It only single user multiple servers. The user forgets a password and not able to access same user name have key value to identify unique values. Once login the entry detail is cannot access the same user name login.

V.CONCLUSION

According this paper tell like a new user security for cloud computing platform includes RSA and encryption algorithm. The user login execution period is not a part of higher.(ie) implementation of each algorithm is perform different servers, and download, upload a files to take overall system is stop difficult. The RSA algorithm and digital signature with encryption model high secured and light encryption system information. We want to work ensure safe communication computers between systems to user.

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. JiyiWu,QianliShen,TongWang,JiZhu,JianlinZhang"Recent Advances in Cloud Security",JOURNAL OF COMPUTERS,vol 6,No 10 ,OCTOBER 2011.
3. RohitBhadauria,RituparanaChaki,NabenduChaki,Sugatasanyal,"A Survey on Security Issues in Cloud Computing",2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

4. VaibhavKhadilkar,AnujGupta,MuratKantarcioglu,LatifulKhan,BhavaniThuraisingham,"Secure Data Storage and Reterival in the c Cloud",University of Texas,2011.
5. Ulf T. Mattsson,"Database Encrption-How to Balance security with Performance",2004.
6. BurtKaliski,The Mathematical of the public key Cryptsystem,RSA Laboratories.
7. "Securing Data at Rest:Developing a Database Strategy"-A While paper for Developers,e-Business Managers and IT
8. KawserwazedNafi,TonnyShekha,kar "new user Authendication Distributed server Based Cloud Computing Security Architecture.
9. Jenson,SchwenkBohali,"Security prospects through clud computing".
10. "Recent Advanced in cloud security" by jiyiwuQianlishenTongwang.
11. "A Privacy preserving Repository for Securing Data across the Cloud"byRanjitemishra.
12. JianchunJiang,WeipingWen,"Information Security issues in cloud computing Environment",Netinfo Security,doi:10.3969/j.issn.1671-1122.2010.02.026.