Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1108 – 1115

SURVEY ARTICLE

SURVEY ON TRIPLE SYSTEM SECURITY IN CLOUD COMPUTING

Parul Mukhi[1], Bhawna Chauhan[2]

[1]M.Tech Scholar, B.S Anangpuria Institute of Technology & Management, Faridabad

[2]Assistant Professor, B.S Anangpuria Institute of Technology & Management, Faridabad

[1] parulmukhi@ymail.com; [2] bhawna.chauhan@faculty.anangpuria.com

Abstract - Large scale distributed systems such as cloud computing applications are becoming very common. These applications come with increasing challenges- how to transfer, where to store and compute data. The most prevalent distributed file systems to deal with these challenges are the Hadoop File System (HDFS) which is a variant of the Google File System (GFS). However HDFS has two potential problems - one is that it depends on a single name node to manage almost all operations of every data block in the file system. As a result it can be a bottleneck resource and a single point of failure. The second potential problem with HDFS is that it depends on TCP to transfer data. As has been seen in many studies TCP takes many rounds before it send at the full capacity of the links in the cloud. This results in low link utilization and longer downloads times. To overcome these problems of HDFS we present a new distributed file system. Our scheme uses a light weight front end server to connect all requests with many name nodes - Triple Security.

Keywords – cryptography; encryption; decryption; data security; key; DSA; AES; STEGANOGRAPHY

I. Introduction

A common understanding of cloud computing is continuously evolving and the terminology and concepts used to define often need the clarification. In common usage, the term "the cloud" is essentially a metaphor for the Internet. Marketers have further popularized the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. remotely through the Internet. Cloud computing was coined for what happens when applications and services are moved into the internet cloud. Like an iphone, Blackberry or Laptop, are using services by thin client or other access point [1].

In short, cloud computing allows for the sharing and scalable deployment of services from almost any location, for which the customer can be charged based on actual usage.

Once a cloud is formed, its cloud computing services are being implemented in terms of business models that can vary depending upon the requirements .The primary service models being created are commonly as follows :

1. Software as a Service (SaaS) — Consumers purchase the ability to access and use an application or service that is being hosted in the cloud. For example - Salesforce.com, where necessary information for the interaction between the consumer and service is hosted as part of the service in cloud. Also, Microsoft is growing up its association in this area.
2. Platform as a Service (PaaS) — Consumers acquire access to the platforms that enable them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the user, and there might be constraints to which applications can be deployed.
3. Infrastructure as a Service (IaaS) — Users control and manage the system in terms of operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure.[1]

II. PROBLEM STATEMENT

Cloud Computing can handle data both in public and private domain. But this apparently undisruptive way of thinking about building applications that has its own set of issues.[3]

The problem is that when cloud service providers provide service, that time the hacker might hack the username and the password. So, to prevent this problem we executed the concept of digital Signature. Digital signatures enable the "authentication" and non-repudiation of digital messages, assuring the recipient of the digital message - both the distinctiveness of the sender and the reliability of the message being sent [1].

III. RELATED WORK

The cloud computing is a practical environment that requires transfer of data right through the cloud. As a result, several data storage concern can take place .In general, users will know neither the exact location of their data nor the other sources of the data collectively stored with them [2]. So, Digital signature algorithm is used to define the authenticity of the data or services that are being provided to the user.

A. DSA (Digital Signature Algorithm)

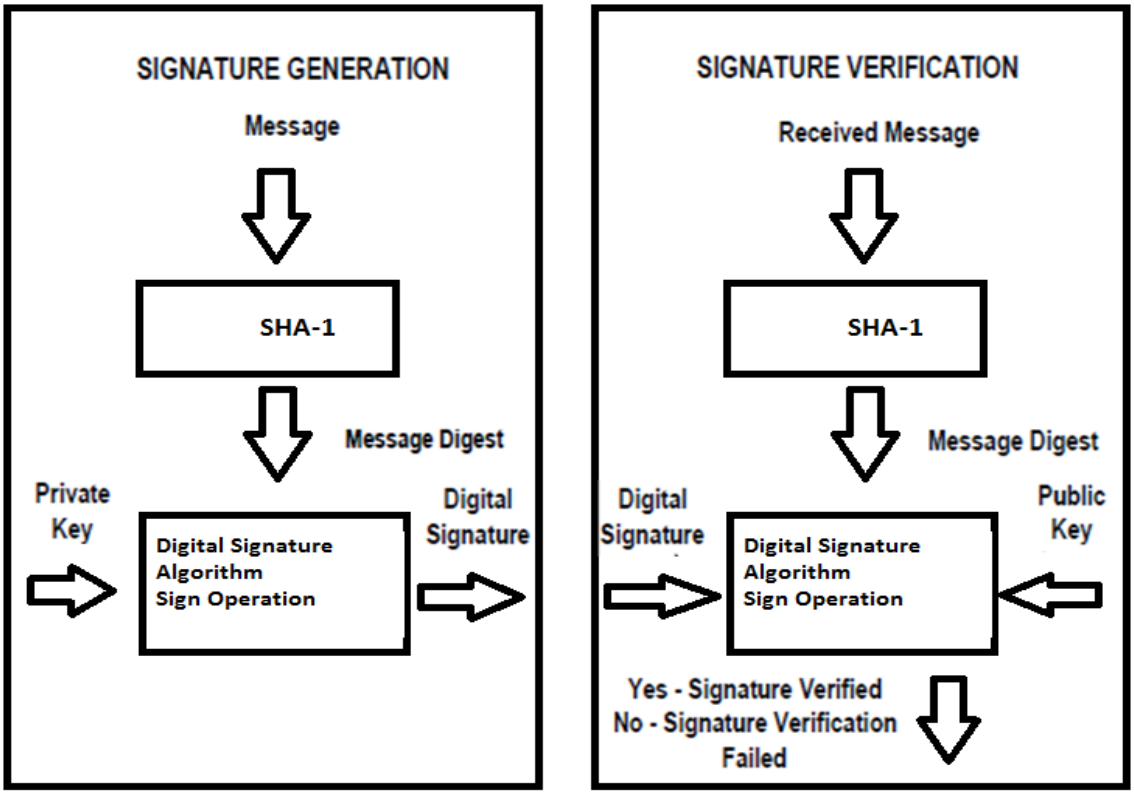
A digital signature algorithm authenticates the integrity of the signed data and the identity of the signatory. A digital signature algorithm may also be used in proving to a third party that data was actually signed by the generator of the signature. Is intended for use in electronic mail, electronic data interchange, software distribution, and other applications that require data integrity assurance and data origin authentication. The wireless protocols, like Hiper LAN/2, and WAP, have specified security layers and the digital signature algorithm have been applied for the authentication purposes. Electronic Signature can prove the Authenticity of Alice as a sender of the

message. **Yuh-Min Tseng a,*, Jinn-Ke Jan b, Hung-Yu Chien b[5]-**proposed a digital signature scheme using self-certified public keys in the ISP era. It provides the message recovery assets. The authenticated encryption scheme only allows a specified receiver to verify and recover the message. The authentic encryption scheme with message linkages is appropriate for the diffusion of large messages, while providing the linkages among signature blocks [1].

a) DIGITAL SIGNATURE ALGORITHM

A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of parameters and authenticates the integrity of the signed data and the identity of the signatory. An algorithm provides the capability to generate and verify signature. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key, which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user public key. Only the possessor of the user private key can perform signature generation.

A hash function is used in the signature generation process to obtain a condensed version of data, called a message digest. The message digest is then input to the digital signature algorithm to generate the digital signature. The digital signature is sent to the intended verifier along with the message. The verifier of the message and signature verifies the signature by using the sender's public key.



B. DES (Digital Encryption Standard)

DES is developed in early 1970s[4] and was designed by IBM and adopted by the U.S.govt.as the standard encryption method. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption and Uses only a single key.S-DES encryption (decryption) algorithm takes 8-bit block of plaintext (cipher text) and a 10-bit key, and produces 8-bit cipher text (plaintext) block. Encryption algorithm involves 5 functions: an initial permutation (IP); a complex function fK, which involves both permutation and substitution and depends on a key input; a simple permutation function that switches (SW) the 2 halves of the data; the function fK again; and finally, a permutation 2 function that is the inverse of the initial permutation (IP-1). Decryption process is similar. The function fK takes 8-bit key which is obtained from the 10-bit initial one two times. The key is first subjected to a permutation P10. Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first sub key (K1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the 2nd sub key K2.

Steps for Proposed Work plan

1. User should not require any third party program to encrypt data on the client side.
2. Every bit of data can read/written to/from the cloud database and must go through an encryption framework.
3. User must be endorsed using passwords, to entrance the data saved on Cipher Cloud.
4. Encryption keys used must be generated instantly and should never be stored on cloud storage framework in any form.
5. Provide an efficient method of encryption over the cloud. [4]

C. Advanced Encryption Standard (AES)

After DES was used as an encryption standard for over 20 years and it was able to be cracked in a relative short amount of time, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place. This decision was announced in January 1997, and a request for AES candidates was made. The AES was to be a symmetric block cipher algorithm supporting keys sizes of 128-, 192-, and 256-bit keys.[5]

The following five algorithms were the finalists:

• MARS Developed by the IBM team that developed Lucifer

• RC6 Developed by the RSA Laboratories

• Serpent Developed by Ross Anderson, Eli Biham, and Lars Knudsen

• Two fish Developed by Counterpane Systems

• Rijndael Developed by Joan Daemon and Vincent Rijmen

By design **AES** is faster in software and works efficiently in hardware. It works fast even on small devices such as smart phones, smart cards etc. **AES** provides more security due to larger block size and longer keys. **AES** uses 128 bit fixed block size and works with 128, 192 and 256 bit keys. Rijndael algorithm in general is flexible enough to work with key and block size of any multiple of 32 bit with minimum of128 bits and maximum of 256 bits. [5]

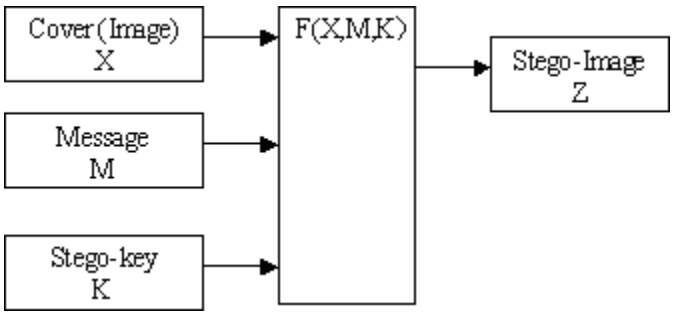
	Triple-DES	**AES**
Description	Triple Data Encryption Standard	Advanced Encryption Standard
Timeline	Standardized 1977	Official standard since 2001
Type of algorithm	Symmetric	Symmetric
Key size (in bits)	168	192
Speed	Low	High
Time to crack (assume a machine could try 255 keys per second - NIST)	4.6 billion years	149 trillion years
Resource consumption	Medium	Low

D. STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Steganography is the process of hiding one medium of communication (text, sound or image) within another. The word Steganography comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and so it literally means, covered writing. [6]

a) Digital Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message [1]. Digital Steganography deals with developing and transmitting digital data/files under the cover of image/pictures. A typical digital steganography encoder is shown in Below Figure. The message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. This is also referred to as the message wrapper. The message embedding technique is strongly dependent on the structure of the cover, and here in this thesis report covers are restricted to being digital images. It is not required that the cover and the message have homogeneous structure. For example, it is possible to embed a recording of Shakespeare's lines (an audio stream message) inside a digital portrait of the famous playwright (an image cover).



b) Audio Steganography (Hiding Data in Audio Files)

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. To put this in perspective, the (HAS) perceives over arrange of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected. There are two concepts to consider before choosing an encoding technique for audio. They are the digital format of the audio and the transmission medium of the audio. There are three main digital audio formats typically in use. They are Sample Quantization, Temporal Sampling Rate and Perceptual Sampling. Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats such as (.WAV and. AIFF). [6]

Algorithm sample
Input: security parameter n, a function g : C ! {0, 1}f , and a value b 2 {0, 1}f
Output: a covertext x
1: j 0
2: **repeat**
3: x R C
4: j j + 1
5: **until** g(x) = b **or** j = n
6: return x [6]

The encoding method is based on an algorithm sample, which samples a covertext according to C such that a given bit string b of length f = O(log |C|) is embedded in it.
The decoding algorithm SD(1n, k, c) outputs m0 Gk(1, c)_Gk(0, c0); it is easy to show that m0 is equal to the message that was embedded using SE except with negligible probability. [6]
Temporal Sampling Rate uses selectable frequencies (in the KHz) to sample the audio. Generally, the higher the sampling rate is, the higher the usable data space gets. The last audio format is Perceptual Sampling. This format changes the statistics of the audio drastically by encoding only the parts the listener perceives, thus maintaining the sound but changing the signal. This format is used by the most popular digital audio on the Internet today in ISO MPEG (MP3) the more popular encoding methods for hiding data inside of audio.

Bender identifies four possible transmission environments .These environments are:

- Digital end-to-end environment
- Increased/decreased resembling environment
- Analog transmission and resembling
- "Over the air" environment

For example, we had an 8 bit audio file with the following values: Decimal form of the audio data: 133 135 136 140 120 100 75 39 In binary, those values would be represented as: Binary form of Audio data: 10000101 10000111 10001000 10001100 0111000 01100100 01001011 00100111 Binary Code of Secret message: 11101101 Now we wanted to hide the binary file 11101101 (237) inside the carrier data. We simply replace the least significant bit in each value (the last value because it will cause the least amount of change in the value as discussed above) by one of pieces of the binary that makes up 213. The modified sequence of binary form of audio file when the secret data 237 is embedded in it is shown below: Binary form of modified carrier data: 10000101 10000111 10001001 10001100 01111001 01100101 01001010 00100111. These new binary values change the values of the audio file very little, with a difference of only one in either direction. These discrepancies are negligible, as humans can't tell the difference at such small levels.

So message is hidden in the audio file. The LSB of the modified image file are extracted to obtain the embedded message.

IV. Overall system Design

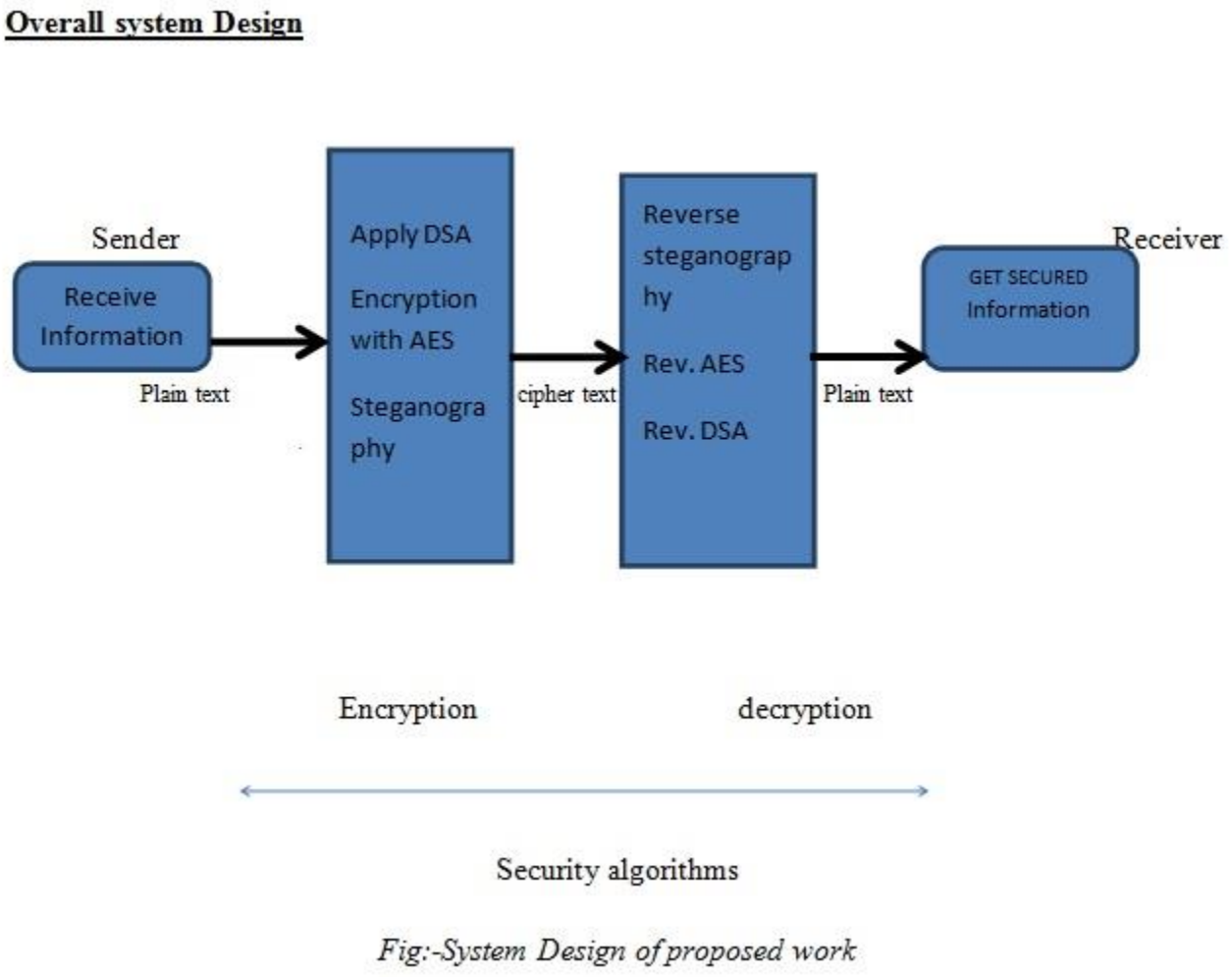


Fig:-System Design of proposed work

V. Conclusion and Future Work

In this , we proposed a model for the truthfulness over cloud computing and we utilize digital signature to achieve the uprightness in such a way that help user to verify and examine the data from unauthorized people that manipulate with the cloud or dig out the data [1]. Another observation that was made is that these days all symmetric/asymmetric encryption algorithms are using hash functions as an integral part for the message integrity [3]. To encrypt large messages an amalgam approach is used in which the messages are actually encrypted using symmetric schemes (DES, AES, etc.) and the key is being transported using asymmetric schemes [3]. Thus, for the future work, we will going to merge all the three algorithms to authenticate the data privacy and hide that text behind a wave file using audio steganography.

REFRENCES

1. Secure Data Storage in the Cloud using Digital Signature Mechanism by Shobha Rajak, Ashok Verma, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.
2. Data Protection Issues in Cloud Computing by Pushpendra Kr. Verma , . Dr. Jayant Shekhar , 2nd International Conference on Role of Technology in Nation Building (ICRTNB-2013) ISBN: 97881925922-1-3.
3. Enhancing Security in Cloud computing using Public Key Cryptography by Birendra Goswami, Dr.S.N.Singh / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 4, July-August 2012, pp.339-344.
4. Using encryption Algorithms to enhance the Data Security in Cloud Computing by MANDEEP KAUR#1, MANISH MAHAJAN#2, International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03 January 2013**ISSN NUMBER : 2278-9723.**
5. Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography , by M.Sudha , M.Monica , Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012 Copyright ©World Science Publisher, United States.
6. Digital Steganography, by Christian Cachin , IBM Research ,Zurich Research Laboratory CH-8803 R¨uschlikon, Switzerland cca@zurich.ibm.com February 17, 2005.
7. U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology-DIGITAL SIGNATURE STANDARD (DSS)
8. Digital signature with message recovery Using self-certified public keys and its variantsYuh-Min Tseng, Jinn-Ke Jan, Hung-Yu Chien
9. YANG Xiaoyuan1, ZHU Shuaishuai, PAN Xiaozhong-
10. Cong Wang, Qian Wang and Kui Ren. ―Ensuring Data Storage Security in Cloud computing‖ 978-1-4244-3876- 1/2009 IEEE.
11. John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―,2009 IEEE CO Published by the IEEE Computer and Reliability Societies.
12. Siani Pearson, ―Taking account of Privacy when Designing Cloud computing Services‖ *CLOUD'09*, May 23, 2009, Vancouver, Canada, 2009 IEEE.

