IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105145

A Study on File Security using Hybrid Cryptography in Cloud Computing

Harikrishna V Holla[1], Nagaraj G Cholli[2]

Student, Information Science and Engineering, R. V College of Engineering, Bangalore, India[1]

Associate Professor, Information Science and Engineering, R. V College of Engineering, Bangalore, India[2]

Abstract: In the past decade cloud computing has been used extensively in industry, personal storage, military, government, etc. Even though storing and accessing data has become a lot easier due to significant development in cloud computing in the last two decades, and there are some issues with increasing dependency on cloud, the biggest issue among many is how secure is data and information in the cloud. So, considering security as priority this paper presents a study on file security using hybrid cryptographic methods. Two of the main constituents of cloud data are text file and multimedia files and here two methods are discussed one each for text file and multimedia file These security issues can be solved using both cryptography and steganography. It can still be improved by using multiple steganography and cryptography techniques.

Keywords: Cryptography, steganography, security, computing, hybrid.

I. INTRODUCTION

Cloud computing is one of the steps in the evolution of the Internet and virtualization, providing all the necessary means for improving and modernising computer infrastructure. Cloud plays a pivotal role in every aspect of computing from application to business processes. Cloud computing explained in simple words is, it can be determined as a set of network, storage, interface, service and hardware that is combined to deliver some aspects of computing as service to users. When it comes to storage of any type, security is very important and that's why there are a set of layers of security protocols present in data storage or data transmission. So, cloud is not much different from classical storage but here all these falls on the company that provides the cloud infrastructure rather than the individual or organization that is using these services.

II. STRATEGIES AND TOOLS

A. Advanced Firewalls

Firewall in cloud is much like traditional firewalls; they manage flow of data between cloud and outside. Since they are a lot more advanced than traditional ones they are also called “Next Generation Firewall” or “Advanced Firewalls”. Most of the Firewalls inspect all the traveling data packets. Simple firewalls just look at the destination and source information of the data packet. Advanced ones look at destination and source and also verify integrity of the packet content. These systems then use this data to map contents to already identified security threats.uy

B. Intrusion Detection

Cloud serves a number of users at the same time so avoiding intruders is important. Intrusion detection is a method used to monitor your server, networks and other IT assets for any policy violation, suspicious activity There are many types of security feature so two important of them are one that stops intruders and other one is when intruder is inside the system, so damage control is important here, so in order to achieve this we need to identify the intruder first so there are multiple level of detection to make sure that the intruder is identified at the earliest and stopped from damaging the data.

C. Event Logging:

Event logging in the cloud is known as cloud logging is an important part of every system but when it comes to cloud computing for security analyst’s logs are the only data. They are also used to reload the last version to restore some lost data. Log gives a lot of data like location which is used to identify if a user is logged in from an unlikely location so we get to know if someone else has access to users account. These logs keep record of all actions in the network, that is who, where and what user did. Analysts can make best use of this data by building a record and predict security breaches

D. Internal firewalls

Internal firewall is a type of security solution that protects the network that has passed through initial defense . One of the important parts of saving a system from falling into the wrong hands is by giving limited access to some of its accounts by using an internal firewall. This boosts security largely. By doing this even if some accounts are compromised, they cannot access all the data. Internal firewalls work by using dual key strategy. Dual strategy here refers to having less attack surface by using micro segmentation, which breaks down networks into zones that are secured independently and by using smart automation to update security based on past activity.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105145

E. Encryption

Encryption as we know is a process of hiding information or data in a code to avoid unauthorized access. Cloud encryption is also similar here files, images, text are transformed before transferring them into the cloud. There are a number of algorithms out there that are being used in this process. It is the simplest and most secure way to make sure that data in the cloud is not accessed by unauthorized persons. Service provider encrypts the data by the best available algorithm and the key is given to the user or customer. Users can use the key to decrypt the data and files as and when required. Even If the attacker gets hold of encrypted data it is of no use. Without the key data is just nonsense.

F. Physical security:

Like any other valuable product, data also needs to be kept in a secure environment. Security doesn't just mean from cyber threats but also physical threats. Physical theft of data has been in place long before virtual threats so securing cloud storage that has data of many organizations and individuals is very important. Physical security can be achieved by heavily guarding cloud data centres, 24-hour CCTV surveillance, biometric locks for authorized personnel, etc.

III. CHALLENGES

A. DDoS and Denial of Service attacks

As most of the businesses are embarrassing the cloud and moving their data into the cloud more and more cloud service providers are being targeted to access personal data of their users. Among several types of attacks, Distributed Denial of Service (DDoS) are severe. Both Platform as a service (PaaS) and software as a service are the two most frequently targeted industries. DDoS attack is an attempt to disrupt servers by overwhelming them. When servers reach capacity, they block any users trying to access so even genuine users are blocked. Due to this the customer's website can go down, his whole business could be stopped. This attack can be on for a few hours and sometimes for days.

B. Data breaches:

Data breach is an incident where sensitive, confidential or protected data is accessed or shared by an unauthorized person. Data breaches have hit an all-time high in India and the world. India is the second most targeted country after the US. There are numerous ways in which data is secured as mentioned above but the security of the data highly depends on the cloud partner or the service provider, because some of them use best available systems to protect data and be vigilant but some of them can be careless so choosing a reliable vendor is very important.

C. Data Loss:

Even though you have moved all your data to the cloud that does not mean total security from data loss. There are tens of ways in which you could lose data like human error, accidental deletion, hardware failure, malware etc. Even though the probability of losing data in cloud storage is way less than losing it in your onsite storage facility, it's not 100 percent safe.

D. Insecure Access Control Points

Cloud is accessible from anywhere with a stable internet connection and a device unlike traditional storage systems. This feature can be a boon and also bane if the interface or application is not secure. As mentioned, if the access point is not secure hackers can get access to the system and exploit it.

E. Notification and alert

Awareness of security issues is an important part of any system. The same goes for cloud systems. Alerting users of data breach as early as the vendor gets to know is really vital for the system to work, because only if the user gets to know about data breach, he can take some measures to control damage or initiate his security and management plan. Sometimes service providers try to hide this information from its customer to hide their lapses but this can become a big loss to both vendor and customer in the future.

IV. RELATED WORK

A. In this paper by KA., LBG., LH., & KA, they have used single key encryption and decryption. There are four steps : authentication, key generation, data encryption and decryption and the process takes place at client end. This paper uses elliptic curve cryptography(ECC) to achieve encryption . ECC is used because it is more efficient than RSA since it uses smaller keys for equivalent security.[1]

B. This paper by R.P., & P.Y. proposed to use Deffiee Hellman key exchange with digital signatures and AES algorithm to improve security in cloud computing. Here Diffie hellman is used to generate a key after that digital signature is used for authentication. Finally AES is used to encrypt files. Whenever the client needs to upload file all three steps take place. And when a client wants to access an uploaded file he will have to go through the same three steps as uploading but in the last step decryption takes place using AES .[2]

C. This paper by Ping, Z. L., Liang, S. Q., and Liang, L. X. implements two encryption that contribute to scalability , high security and easy accessibility. This can be implemented for multimedia content on the cloud. The two encryption used are RSA and MD5. RSA for key generation and MD% for encryption and decryption. [3]

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105145

D. In this paper by Rawal, B. S., & Vivek, S. S they have used three different servers for data storage, used input and user output. So even if one of the servers fails the system does go down but a certain functionality of the system will be down depending on which server is down. User input server is used to authenticate and input data. Data storage server receives file from input server and it encrypts using AES algorithm and it is sent to user output server . Output server sends the decrypted file back to the user when requested.[4]

Table I. COMPARISON OF RELATED WORKS

No	Title	Method	Impediment
1	Secure storage and access of data in Cloud computing.	Uses ECC (Elliptic Curve Cryptography) encryption algorithm. Has four steps, Performs authentication, key generation, encryption and decryption.	Only one encryption technique is used. ECC is not secure enough to perform all the encryption and key authentication
2	Use of Digital Signature with Diffie Hellman key exchange and AES encryption algorithm to enhance Data Security in Cloud Computing.	Diffe Helman is used for key exchange. Digital Signature is used for Authentication and AES is used for file encryption.	Since three cryptographic methods are used to perform different actions it can be time consuming
3	RSA Encryption and Digital Signature.	RSA and MD5 algorithms are used here to achieve data security	Since MD5 algorithm is used it can only provide with single text encryption and not multiple text encryption
4	Secure File Storage and File Sharing.	Uses 3 different servers for upload, store and download files. Better than single server model	Sometimes connectivity issues between servers can be an issue.

V. HYBRID CRYPTOGRAPHY

All the present cryptography methods are decades old so using a single cryptography method won't be of any use since there are many work arounds for the hackers. So in order to overcome this hybrid cryptographic methods are used. In this paper two of the important methods will be discussed. The first method is for text encryption, so as to provide better options to users there are two options, approach 1 uses RSA and AES and approach uses AES and Blowfish Second method uses AES, RC6, Blowfish and BRA. Method 1 is mainly used for multimedia encryption and method 2 for text file encryption.

A. METHOD 1

How the system works

- User can login if he is already registered otherwise he will have to sign up.
- Users will have to select files to be uploaded.
- User can select the combination of encryption algorithm that is AES and Blowfish or AES and RSA
- Then later the file is uploaded and encrypted.
- To access or download their file, users will have to enter a key sent to them in mail.
- This system provides two layers of security. Secure user login acts as a first layer and encryption of file acts as a second layer of security. When encryption takes place a unique key generated which is sent to user email entered when signing up. User will have to enter that key to access the file.[6]

AES algorithm

Advanced Encryption Standard is a symmetric key block cipher. It has three 128 bit block ciphers. AES does not depend on the Data Encryption Standard(DES) feistel network. AES is faster and better than DES. Figure 1 shows the working of AES.

Algorithm

Initial step:Add round key- This is done by using XOR. Each byte with a block of round key

Rounds

1. Sub bytes: By using a look up table or S-box each byte is replaced . This results in a matrix of 4 rows and 4 columns
2. Shift row: Each row is circular left shifted incrementally according to row number.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105145

3. Mix column:Using a special mathematical function each column is transformed
4. Add round key: Similar to the initial step, each byte is XOR with a 128 bit round key.

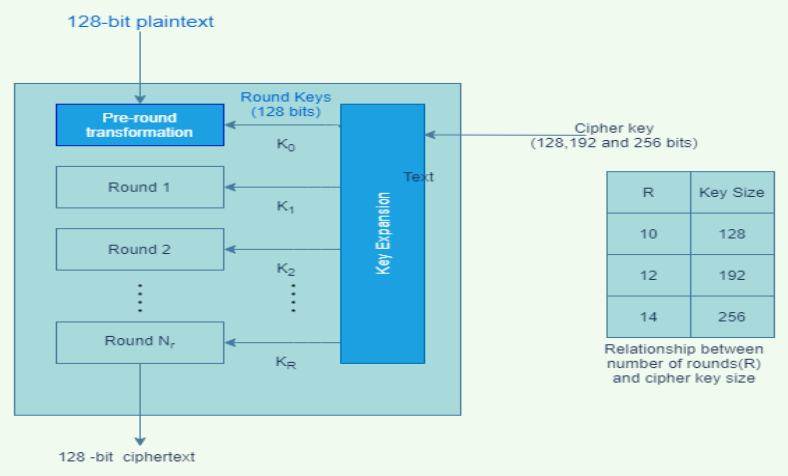

Fig. 1 AES Algorithm

Blowfish algorithm

Blowfish algorithm is a symmetric encryption which uses the same key for encryption and decryption.It is also a block cipher which means it encrypts data in a blocked manner. Blowfish algorithm uses XOR lookup table with 32 bit operands. Key length may vary from 32 upto 448 bits.Here in this algorithm each block has 64 bits. It uses a 16 round feistel network. Figure 2 shows working of blowfish algorithm

It has two parts

- Key - expansion
- Data encryption

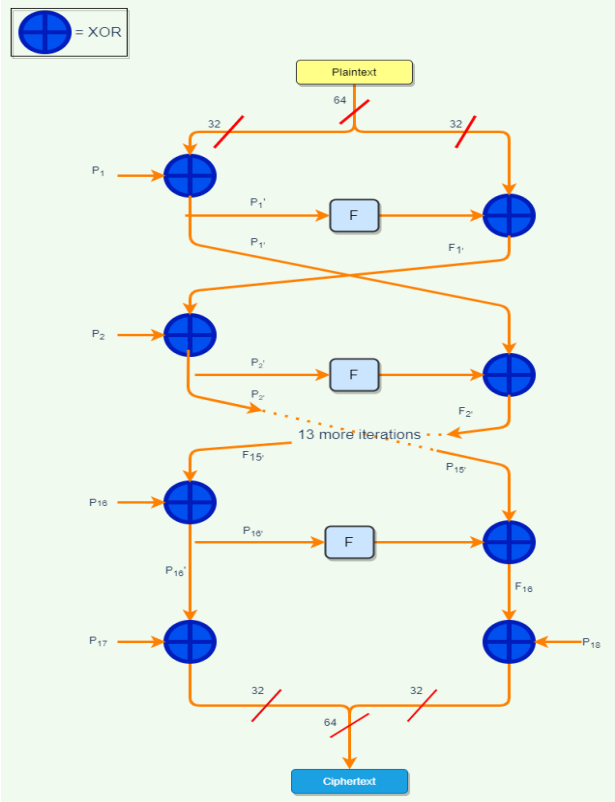

Fig. 2 Blowfish Algorithm

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105145

RSA algorithm

RSA stands for Rivest-Shamir-Adleman algorithm, It is a secure public key cryptographic method. This method uses two large prime numbers p and q to encrypt data. There are three more integers n,d and e that are derived from p and q which serve as public and private keys. Figure 3 shows the working of the RSA algorithm.

- n is product of p and q
- d is a large integer such that GCD of d and (p - 1)*(q - 1) is 1
- e is a value such that e * d=1(mod((p - 1) * (q - 1)))

Here (e,n) is public key and (d,n) is private key

- Large messages are broken into small blocks and are given a number in range 0 to n-1.
- Raise the message to eth power modulo n which gives cipher text.
- By raising ciphered text to dth power modulo n.

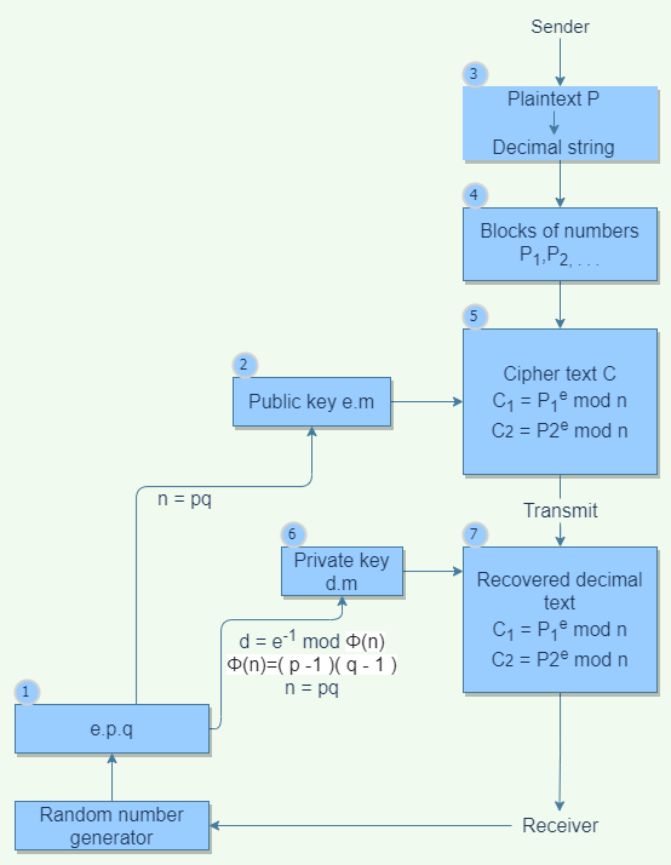

Fig. 3 RSA Algorithm

This system uses a two stage encryption process. It can be AES and RSA or AES and Blowfish algorithms. This system increases scalability, security, confidentiality and easy accessibility. Here a randomly generated key is used so it's more secure than conventional encryption. For the decryption process the user will have to enter a key generated while encryption and send his/her email.

B. METHOD 2

This method uses Blowfish, AES, RC6 and BRA algorithms to provide block wise security, All the above algorithms use 128 bit key size.Since different parts of file is using different parts file is encrypted using different algorithm we must make sure which part is encrypted using which algorithm and also which part uses which key so in order to achieve this Least Significant Bit (LSB) method is used. LSB encrypts the key in an image of the file. Normally a file is divided into four or eight parts but it can be divided into a number of parts and using a round robin method each part can be encrypted using one of the algorithms.[5]

Advantages of hybrid cryptography for text file

- Uses 17%- 20% less time as compared to AES
- AES need 15% to 17% more time for file decryption as compared to hybrid system

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105145

- Hybrid system performs 13% better than blowfish algorithm while encrypting
- Blowfish take 10% to 12% more time to decrypt file[5]

VI. CONCLUSION

This study focuses on file security in cloud computing and also gives a brief idea about all the challenges and systems present in order to avoid any malicious activity. This paper goes through few of the previous works and then also briefly explains two methods used in securing multimedia and text files . As already mentioned, having double encryption for multimedia will increase its security against many threats mentioned above. And for text files as technology has improved a lot since encryption algorithms were designed there's a good chance even double encryption could be cracked so multiple encryption with LSB to hide key in image format. So by this we can say that both multimedia and text files can be sufficiently secured using above hybrid algorithms such that even if an unauthorized person gets hold of the file it will be impossible to crack and get hold of sensitive data and since multithreading is used this algorithm is faster than traditional.

REFERENCES

[1]. Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).
[2]. Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.
[3]. Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.
[4]. Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).
[5]. P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 1635-1638, doi: 10.1109/WiSPNET.2016.7566416.
[6]. Shruti Kanatt , Prachi Talwar , Amey Jadhav, 2020, Review of Secure File Storage on Cloud using Hybrid Cryptography, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 02 (February 2020),
[7]. V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm," 2014 International Conference on Power, Automation and Communication (INPAC), 2014, pp. 146-149, doi: 10.1109/INPAC.2014.6981152.
[8]. P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 437-439, doi: 10.1109/CSNT.2013.97.
[9]. Mohamed, N.N. & mohd yussoff, Yusnani & Saleh, Mohd.A. & Hashim, Habibah. (2020). HYBRID CRYPTOGRAPHIC APPROACH FOR INTERNET OF THINGS APPLICATIONS: A REVIEW. Journal of Information and Communication Technology. 19. 279-319. 10.32890/jict2020.19.3.1.