International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Secure File storage on Cloud Computing using Hybrid Cryptography Algorithm

Aishwarya S. Dashmukhe and Nilesh Alone

Department of Computer Engineering GESRH Sapat college of engineering

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Cloud Computing is very famous and flexible Technology which is used in many areas like Industry,Military, Education,Hospitals,Telecommunication etc to store large amount of data. This data access by user very quickly as per request of user, but there is many issue to store data on cloud regarding security because number of user shear same data. The basic Aim to design security method by using Hybrid Cryptography to provide a highest level of security. Provide highest level security by using single algorithm it is difficult. In this paper we try to introduce new cloud computing security by using Symmetric key cryptography algorithm and stenography. In proposal system AES, Blow-fish, RC6, BRA algorithms are included for security purpose. All algorithms have 128bit key size and file divide into Eight parts and each and every part will be encrypted with the help of Multi threading technique. key for data encryption is covered in Image using LSB technique. Image is send to Valid Reviver using mail for the Decryption purpose.

Keywords: *Cloud services, Encode, Decode, Hybrid Cryptography,steganography,Blowfish,RC6 and BRA.*

Introduction

Now a day's cloud computing is most powerful technology which is manage all information and application its provide resource like software, Application, and Services to customers. Cloud computing is cost saving technology to use for any purpose. Basically cloud computing is a Internet based serious which allow to user shear data, Information, files ect as per demand but security is most important part of this data storage technique. Number of people shear a same data on same cloud for that purpose provides a higher level of security is a major role.

a) Cryptography technique translate original data into unreadable format its divide into symmetric key cryptography and Public key cryptography both technique used to translate data into unreadable format. Data access only by Authorized person as per request. In symmetric key cryptography algorithm some following algorithm are included like DES,AES,3DES,IDEA,BRA, Blow-fish Public key cryptography algorithm are REA and ECC. Public key and Private key are manipulate in public key cryptography algorithm. This algorithm are Incised level of security at the time of encoding and decoding. Stenography hide data original data is only accessible to authorized person. It Increased level of security after adding data into text cover file its look like a normal file if any unauthorized persona try to catch that data then it is not possible to access and it tack time because of DES algorithm is used for this data encoding and decoding. Image stenography basically used LSB technique. In LSB stenography technique we can store a larger amount of data with good security. AES is a cryptography algorithm with support three type of key 128 bit, 192 bit and 256 bit, AES algorithm provide higher level of security for image and better performance.

b) Image stenography used three bit LSB technique sen-sitive data hide in image. We can hide large amount of data into Image stenography AES is symmetric key cryptography algorithm. It supports three types of keys. For 128 bit,192 bit and 256 bit encryption and decryption time is reduced .Advantage of modified AES algorithm is provides better performance. Symmetric key cryptography algorithm is applies a single key for texts encode and decode for Size of key is 128 bit. This algorithms have many different steps randomly so unauthorized person can not use data. data encode purpose two keys are used. DES algorithm128 bit input of is divided into two parts .That two parts are executed at a same time.DES algorithm has one weakness. That is less key size.3DES algorithm essential large amount of time for encryption and decryption .Improved DES algorithm have capability of provide better performance as compare to DES and 3DES Name Based Encryption Algorithm is work on one byte at a time. uses secret key for

encryption and decryption .Key generation process is done using random key generation technique.

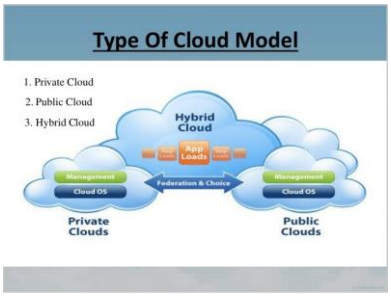

Fig. 1. Types Of Clouds)

c) Disadvantage of algorithm is it tack maximum time for converting data into cipher text because it operate on single byte at a time To solve data storage and security issues author has new security model The main about this system to reduce the higher cost and Provide better security .Private cloud is more secure than the public cloud .Source file upload on cloud and divide into different format. Every part of file is encrypted and stored on more than one cloud. Information about file is stored on cloud server for decryption purpose. If attacker or unauthorized people try to catch original data they are not able use the same data.:

Review of Literature

In existing system single algorithm used for data encode and decode purpose, But use of single algorithm is not effective provide high level security. If we use single symmetric key cryptography algorithm than we have to face so many security issue because in this type of algorithm applies a single key for data encode and decode. Public key cryptography algorithms accomplish high security but take maximum time for data encode and decode. To solve above issues we have introduced new security mechanism which is hybrid cryptography.

a) In the paper "Ensuring Data Storage Security in Cloud Computing" authors Cong Wang, Qian Wang, and Kui Ren focused on data security in cloud which is an important quality of service. To provide data security they proposed a scheme for which provides data security and data manipulation.:

b) In the paper "Research on Cloud Computing Security Threats using Data Transmission", the author Raj Kumar focused on cloud computing security. The security is based on encryption and decryption techniques.:

c) In the paper titled "Big Data Analytics: Security and Privacy Challenges" authors Youssef Gahi, Mouhcine Guennoun, Hussein T. Mouftah Focused on big data security and privacy challenges.

In the paper "Toward a Big Data Architecture for Security Events Analytic" the authors Laila Fetjah, Karim Benzidane, Hassan El Alloussi, Othman El Warrak, Said JaiAndaloussiand Abderrahim Sekkaki focused on scalable module which is based on big data techniques and tools which provides solution to process and analyse events like packet flow, log file to generate informative decisions.:

d) The paper entitled "Survey of Big Data Information Security" the authors Natalia Miloslavskaya and Aida Makhmudova focused on big data security features by using big data mining algorithm which are formulated based on IS properties. The paper titled "A Space-and-Time Efficient Technique for Big Data Security Analytics" the authors Suliman A. Alsuhibany focused on space and time efficient probabilistic technique called bloom filter (BF) which contributes to the network security domain. :

Proposed Work

This section contains information regarding to work about system. For hybrid Cryptography AES and RSA algorithms used .AES algorithm require a single key but In hybrid algorithm we used three keys. For data upload on cloud mandatory keys are AES secret key and RSA public key. Private key of RSA and AES secret key are essential to download data from cloud. Whenever use makes an effort to upload data on cloud first that file stored onto directory for short time. In encryption process first AES algorithm is applied on file after that RSA algorithm is applied on encrypted data. Reverse process is followed for decryption. After applying keys that file covert into encoded form and stored on cloud server.

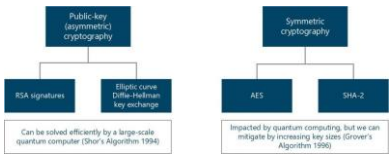

Fig. 2. Cryptography technique)

a) Data security is very important thing for providing quality of service. The two challenges that are Cloud Computing inevitably pose new challenging security threats for number of reasons 1. Firstly, Users have different kinds of data that needs to be stored in cloud and data security is very important and correctness of data needs to be ensured. 2. Secondly, the users will not use cloud for only storing the data. They are frequently accessed or manipulated by the users.:

Methodology

Encryption: encryption Process Basic function of this project is to encrypt the user data to protect data from unauthorized access or hackers in cloud at the time of data transmission also. After encryption data will convert into cipher text this data is not in readable format . Select a secret key K between the ranges of 448 bits to 1024 bits of variable length. Encrypt the

selected file f, by applying Blowfish algorithm with the help of secret key. Blowfish algorithm is a symmetric key cryptographic algorithm, which uses single key to convert the original data into cipher data and vice versa. This key is known as secret key or private key. It has a 64 bit block size and the length of key is from 32 bits to 448 bits. Ef = EBK(f)

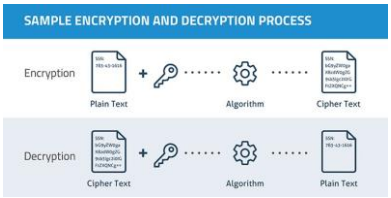

Fig. 3. Encryption and Description

For example: Encrypt the secret key K, using RSA algorithm. RSA algorithm is an Asymmetric key cryptographic algorithm, which uses pair of key for encryption and decryption. EK = ER(K) iv) Apply SHA 2 on encrypted file Ef to generate message digest or hash code. SHA stands for Secure Hash Algorithm, which is used to generate the message digest. Md = S(Ef)
Apply digital signature algorithm on message digest to generate digital signature. Ds = D(Md)
K= DR(EK)
For example: To get the secret key K, decrypt the encrypted secret key EK by applying RSA decryption algorithm.
K= DR(EK)

Fig. 4. Level of encryption

Using above secret key, obtain the original file f, by applying blowfish decryption algorithm on encrypted file Ef. f = DBK (Ef) Apply verification algorithm of digital signature on digital signature on ds to get the expected message digest or hash code. M d = V(Ds)Compare this message digest or hash code with the SHA 2 generated message digest or hash code. M d = S(Ef)]Decryption: In decryption process cipher data is converted into original data. In this cryptography method first phase is hybrid decryption phase and second phase is signature verification phase. Hybrid decryption phase is a reverse process of hybrid encryption phase. This phase is responsible for decryption of encrypted message with the help of RSA and Blowfish. First step, RSA decryption algorithm decrypts the encrypted key, which helps to get original data. Second step, with the help of decrypted key blowfish decryption algorithm decrypt the encrypted data. To get the secret key K, decrypt the encrypted secret key EK by applying RSA decryption algorithm.
K= DR(EK)
For example: To get the secret key K, decrypt the encrypted secret key EK by applying RSA decryption algorithm.
K= DR(EK)
Using above secret key, obtain the original file f, by applying blowfish decryption algorithm on encrypted file Ef. f = DBK (Ef) Apply verification algorithm of digital signature on digital signature on ds to get the expected message digest or hash code. M d = V(Ds)

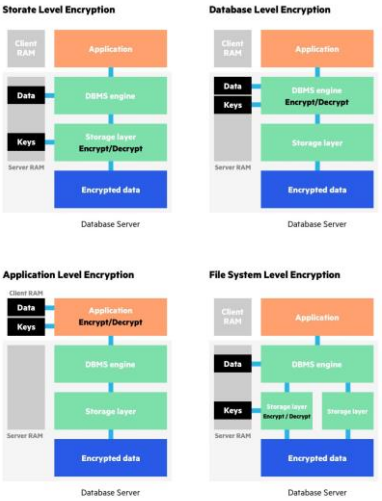

Fig. 5. Level of encryption

Compare this message digest or hash code with the SHA 2 generated message digest or hash code. M d = S(Ef)

a) Data record in the cloud: A data record is can bea document, Business records which may include meeting minutes, memorandum, employment contracts, and accounting source documents, student record, patient record etc. It must be retrievable at a later date so that the data can be accurately reviewed as required. Data which are stored in cloud are also named as a resources in cloud.

b) Data Storage : Data has come to prominence withindata domain as a tool to help users work more efficiently and streamline the collection and distribution of Information Technology. These resources are well managed in Cloud with efficient scalability. Data can be user or server Credentials.:

c) Big-data processing: The stored data are retrieved from Authorized client or server. Admin enables respective client to access the resources based on the user IP provided. When hackers information's are

updated these information are also stored as a resource but it will be encrypted. Only admin can decrepit.:

d) Big-data Development: Based on user malicious activities the admin block or remove the Client IP, such clients are Hackers. The lists of hackers are stored in Hackers Information, which makes ease of work to admin by auto sending alert mail to admin.:

Conclusion

a) In the current paper the problem of data security on cloud data storage has been most important issue. To ensure the correctness of client data in cloud data storage, the proposed method encrypts data and stores it in cloud and user is allowed for modification of data. Cloud storage issues are solved using cryptography and stenography techniques. Block wise Data security is achieved using AES, RC6, Blow-fish and BRA algorithms.

Key information security is accomplished using LSB technique. Data integrity is accomplished using SHA1 hash algorithm. Low delay parameter is achieved using multi threading technique. With the help of proposed security mechanism data integrity, high security, low delay, authentication and confidentiality parameters are accomplished In future, try to accomplish high level security using hybridization of public key cryptography algorithms. Basically this work reduces number of hackers to hack the resources. But the performance has to be increased when number of users are more and access time efficiency should be well managed. As part of future work it can be enhanced to provide supporting features such as Auto mail of restricting IP to client and Deploying in real world environment.:

References

[1]. Cong Wang, Qian Wang, and Kui Ren," Ensuring Data Storage Security in Cloud Computing", US National Science Foundation,2015, pp1-4.

[2]. Kumar, "Research on Cloud Computing Security Threats using Data Transmission" International Journal of Advanced Research in Computer Science and Software Engineering, India Volume 5, Issue 1, January 2015, pp. 399402.

[3]. Youssef Gahi, Mouhcine Guennoun, Hussein T. Mouftah, "Big Data Analytics: Security and Privacy Challenges", IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, June 2016, pp 15-17.

[4]. Laila Fetjah, Karim Benzidane, Hassan El Alloussi, Othman El Warrak,Said Jai- Andaloussi," Toward a Big Data Architecture for Security EventsAnalytic", IEEE 3rd International Conference on Cyber Security and Cloud Computing , Beijing, China,2016,pp 1-7.

[5]. Natalia Miloslavskaya and Aida Makhmudova, "Survey of Big Data Information Security", 4th International Conference on Future Internet of Things and Cloud Workshops, Vienna, Austria, Aug 2016,pp 4-9.

[6]. Suliman A. Alsuhibany," A Space-and-Time Efficient Technique for Big Data Security Analytics", vol. 46, no. 2, Riyadh, Saudi Arabia ,pp.241-284, 2016.

[7]. V.S. Mahalle , A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa Aes) Encryption Algorithm", IEEE , INPAC,pp 146-149,Oct .2014

[8]. Abu Marjan, Palash Uddin, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography",IEEE, IFOST,pages 14-17, October 2014.

[9]. P. S. Bhendwade and R. T. Patil, "Steganographic Secure Data Communication",IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014

[10]. S. Hesham and Klaus Hofmann , "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE,International Symposium on Design and Diagnostics of Electronic Circuits Systems, pages 167170,April 2014.

[11]. M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput",IEEE, ICCCI ,pages 1-5,January 2014.

[12]. S. Ali Abbas, " Enhancing the Security of Identity and Access Management in Cloud Computing using Elliptic Curve Cryptography", IJERMT , Volume-4, Issue-7,ISSN: 2278-9359 ,pages 8-15,2015.

[13]. N. Sharma ,A.Hasan, "A New Method Towards Encryption Schemes(Name-Based-Encryption Algorithm)",IEEE, International Conference on Reliability, Optimization and Information Technology,pages 310-313,Feb