Scientific Journal Impact Factor (SJIF) : 4.364
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

ENHANCING SECURITY SOLUTIONS WITH COLLABORATIVE CRYPTOGRAPHY AND DIGITAL SIGNATURE SCHEME IN CLOUD SERVICES

Ms. S. Meena[1] and Dr. N. Kowsalya[2]

[1]*M.Phil Full time Research Scholar, PG& Research Department of Computer Science, Vivekananda College of Arts & Sciences for Women (Autonomous), Namakkal-637 205,Tamil Nadu, India*

[2]*Asst. Professor, PG& Research Department of Computer Science &Applications Vivekananda College of Arts & Sciences for Women (Autonomous), Namakkal-637 205,Tamil Nadu, India*

Abstract-The cloud computing environment provides storage spaces for the shared data operations. The cloud file storage security is provided with Hybrid Cryptography technique. The Hybrid Cryptography technique integrates the Advanced Encryption Standard (AES), Blowfish, Rivest Cipher 6 (RC6) and Byte rotation algorithm (BRA) based symmetric cryptography methods. The data file is divided into 8 segments and each segment is encrypted with a secret key cryptography algorithm. The encrypted file is transferred to the cloud user with reference to the request value. The image steganography is employed to transfer the key values to the cloud users. The encrypted cloud services are build with Collaborative Cryptography and digital signature techniques. The collaborative cryptography model combines the symmetric and asymmetric cryptography algorithms. The RSA and Elliptic Curve Cryptography (ECC) algorithms are applied to improve the security levels. The Key Distribution Center (KDC) is build to manage the key distribution activities with image steganography technique. The digital signatures are used to verify the data transmission operations. The Message Digest 6 (MD6) Algorithm is adapted for the data integrity verification process.

Keywords-Encrypted cloud services, Hybrid Cryptography, Collaborative Cryptography, Key Distribution Center and Digital signature

I. INTRODUCTION

Cloud computing security, performance and availability are three hot spots of the cloud computing research. And cloud computing security is at the top of them. Based on the three different definitions of cloud computing such as IaaS, PaaS and SaaS, cloud computing can be divided into three levels: the infrastructure layer, platform services layer, application layer software. The security issues of the three levels are different. Data center construction, physical security, network security, transport security and system security is the key point for IaaS. However, for PaaS, data security, data availability, computing availability and the problems of disaster and recovery are paid more attention to. To the highest level of SaaS, the problems of data and application security are gained more attention. Furthermore, when SaaS is constructed on the platform of the cloud computing, most of these security issues on the highest layer are unknown and uncontrollable.

Cloud computing data security is the key component of cloud computing security and important means to ensure the cloud computing popular. Cloud computing migrates data and software to Mega-data centers, this state data and service management are not completely trusted by users. The new character brings a lot of new security challenges which have not been taken into account completely in the current cloud computing system. As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. In this article, the cloud computing technology architecture and the cloud computing data security features are the

Volume 04, Issue 9, [September– 2017] ISSN (Online):2349–9745; ISSN (Print):2393-8161

first to be studied and considered, then the cloud computing data security model is raised. At last, the realization of data security model has been researched.

For data security, in addition to the traditional client - side security, communication security, the security of master - slave structure and other security threats, for some kinds of reasons, cloud computing data lead to new security threats are inevitably led to by cloud computing data. There are several aspects as follows, classified threat of failure, dynamic integrity threats distributed availability threats.

II. RELATED WORK

In this subsection, we describe a classification of PEKS schemes based on their security.

A. Traditional PEKS.

Following Boneh et al.'s seminal work, Abdalla et al. formalized anonymous IBE (AIBE) and presented a generic construction of searchable encryption from AIBE. They also showed how to transfer a hierarchical IBE (HIBE) scheme into a public key encryption with temporary keyword search (PETKS) where the trapdoor is only valid in a specific time interval [8]. Waters the PEKS schemes based on bilinear map could be applied to build encrypted and searchable auditing logs. In order to construct a PEKS secure in the standard model, Khader proposed a scheme based on the k-resilient IBE and also gave a construction supporting multiple-keyword search. The first PEKS scheme without pairings was introduced by Di Crescenzo and Saraswat. The construction is derived from Cock's IBE scheme is not very practical.

B. Secure Channel Free PEKS.

The original PEKS scheme requires a secure channel to transmit the trapdoors. To overcome this limitation, Baek et al. proposed a new PEKS scheme without requiring a secure channel, which is referred to as a secure channel-free PEKS (SCF-PEKS). The idea is to add the server's public/private key pair into a PEKS system. The keyword ciphertext and trapdoor are generated using the server's public key and hence only the server is able to perform the search. Rhee et al. later enhanced Baek et al.'s security model for SCF-PEKS where the attacker is allowed to obtain the relationship between the non-challenge ciphertexts and the trapdoor. They also presented an SCF-PEKS scheme secure under the enhanced security model in the random oracle model. Another extension on SCF-PEKS is by Emura et al. [5]. They enhanced the security model by introducing the adaptively secure SCF-PEKS, wherein an adversary is allowed to issue test queries adaptively.

C. Against Outside KGA.

Byun et al. introduced the offline keyword guessing attack against PEKS as keywords are chosen from a much smaller space than passwords and users usually use well-known keywords for searching documents. They also pointed out that the scheme proposed in Boneh et al. was susceptible to keyword guessing attack. Inspired by the work of Byun et al., Yau et al. demonstrated that outside adversaries that capture the trapdoors sent in a public channel can reveal the encrypted keywords through off-line keyword guessing attacks and they also showed off-line keyword guessing attacks against the (SCF-)PEKS schemes. The first PEKS scheme secure against outside keyword guessing attacks was proposed by Rhee et al. In [2], the notion of trapdoor indistinguishability was proposed and the authors showed that trapdoor indistinguishability is a sufficient condition for preventing outside keyword-guessing attacks. Fang et al. [6] proposed a concrete SCF-PEKS scheme with KGA resilience. Similar to the work in [5], they also considered the adaptive test oracle in their proposed security definition.

D. Against Inside KGA.

Nevertheless, all the schemes mentioned above are found to be vulnerable to keyword guessing attacks from a malicious server. Jeong et al. showed a negative result that the consistency/correctness of PEKS implies insecurity to inside KGA in PEKS. Their result indicates that constructing secure and consistent PEKS schemes against inside KGA is impossible under the

Volume 04, Issue 9, [September– 2017] ISSN (Online):2349–9745; ISSN (Print):2393-8161

original framework. A potential solution is to propose a new framework of PEKS. In [10], Peng et al. proposed the notion of Public-key Encryption with Fuzzy Keyword Search (PEFKS) where each keyword corresponds to an exact trapdoor and a fuzzy trapdoor. The server is only provided with the fuzzy trapdoor and thus can no longer learn the exact keyword since two or more keywords share the same fuzzy keyword trapdoor. Their scheme suffers from several limitations regarding the security and efficiency. Although the server cannot exactly guess the keyword, it is still able to know which small set the underlying keyword belongs to and thus the keyword privacy is not well preserved from the server. Their scheme is impractical as the receiver has to locally find the matching ciphertext by using the exact trapdoor to filter out the non-matching ones from the set returned from the server.

III. ENCRYPTED CLOUD SERVICES WITH HYBRID CRYPTOGRAPHY ALGORITHM

Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.

Symmetric key cryptography algorithms are AES, DES, 3DES, IDEA, BRA and blowfish. The main issue is deliver the key to receiver into multi user application. These algorithm require low delay for data encode decode but provides low security. Public key cryptography algorithm is RSA and ECC algorithm. Public and private keys are manipulated into public key cryptography algorithms. These algorithms accomplished high level security but increase delay for data encode and decode. Steganography hide the secret data existence into envelope. In this technique existence of data is not visible to all people. Only valid receiver knows about the data existence. Text steganography technique is used to produce high security for data. Secret data of user hide into text cover file. After adding text into text cover file it looks like normal text file. If text file found by illegitimate user than also cannot get sensitive data. If illegitimate user try to recover original data than large amount of time is essential.DES algorithm is used for text encode and decode. Advantage of text steganography technique is provide security to text. Minimum space is essential for text steganography as compare to image steganography.

Three bit LSB technique used for image steganography. This system is suggested by author R.T.Patil .Sensitive data of user hide into cover image. We can hide huge amount of into image using LSB steganography technique .The author Klaus Hafmann has implemented high throughput architecture for cryptography algorithm.AES is symmetric key cryptography algorithm. It supports three types of keys. For 128 bit key require 10 rounds, 192 bit key require 12 rounds and 256 bit key require 14 rounds. In improved AES algorithm encryption and decryption time is reduced .Advantage of modified AES algorithm is provides better performance in terms of delay.[3][4]

New symmetric key cryptography algorithm is presented by author M. Nagle. It applies a single key for texts encode and decode. Size of key is 128 bit. Many steps are executed randomly so illegitimate user can even guess the steps of algorithm. Provide high throughput is one of the advantage of symmetric key cryptography algorithms. Improved DES algorithm uses 112 bit key size for data encode and decode. For data encode purpose two keys are used.128 bit input of DES algorithm 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 has capability of provide better performance as compare to DES and 3DES. Name Based Encryption Algorithm is work on one byte at a time. It uses secret key for encryption and decryption .Key generation process is done using random key generation technique. It provides security to data. Disadvantage of this algorithm is essential maximum time for converting data into cipher text because it operate on single byte at a time [7]. To solve data storage and security issues author has new security model .In this model private and public cloud storage areas are used for increase security level of data. On private cloud secure data is stored and unnecessary data is stored on public cloud. Because public cloud any one can access. The main reason behind this system is reduce storage cost .Private cloud is more secure than the public cloud.

Volume 04, Issue 9, [September– 2017] ISSN (Online):2349–9745; ISSN (Print):2393-8161

To enhance security of file in cloud computing .Source file is break into different into different part. 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 tries to recover original file than t he will get only a single part of file. Elliptic Curve cryptography algorithm is used to accomplish high level security .Key managing complications are removed using access management and identity.ECC algorithm need maximum amount of time for file encode and decode. File is converted into unreadable format using AES algorithm. Encrypted file is stored on cloud.AES algorithm is less secure than public key cryptography algorithms.

AES and 3DES algorithms are merge into hybrid algorithm to accomplish confidentiality. It is harder for attacker to recover secret file of user. It consumes maximum amount of delay to translate data into decode and encode form. In existing system single algorithm is used for data encode and decode purpose. But use of single algorithm is not accomplish high level security. If we use single symmetric key cryptography algorithm than we have to face security problem because in this type of algorithm applies a single key for data encode and decode. So key transmission problem occur while sharing key into multiuser environment. Public key cryptography algorithms accomplish high security but maximum delay is needed for data encode and decode. To solve above issues we have introduced new security mechanism.

Cloud owner and cloud user are included into system architecture. Cloud owner upload the data on cloud server. File is split into octet. Every part of file is encoded simultaneously using multithreading technique. Encoded file is stored on cloud server. Keys used for encryption are stored into cover image. Cloud computing is the multi user environment .In this more than one user can access file from cloud server. Cloud user request for file. On request of file user also get stego image using email which consist of key information. Reverse process is used for decode the file.

IV. ISSUES ON HYBRID CRYPTOGRAPHY SCHEME

The cloud file storage security is provided with Hybrid Cryptography technique. The encryption/decryption operations are performed with 128 bits key based symmetric cryptography methods. The Hybrid Cryptography technique integrates the Advanced Encryption Standard (AES) and Blowfish algorithm. The Rivest Cipher 6 (RC6) and Byte rotation algorithm (BRA) are also combined in the Hybrid Algorithm. The data file is divided into 8 segments and each segment is encrypted with a secret key cryptography algorithm. The encrypted file is transferred to the cloud user with reference to the request value. The image steganography is employed to transfer the key values to the cloud users. The Least Significant Bit (LSB) encoding scheme is used for the image steganography. The following issues are identified from the current encrypted cloud services.

- Data integrity verification is not supported
- Public Key Infrastructure (PKI) models are not focused
- Key leakage control is not provided
- Computational and communication complexity is high

V. COLLABORATIVE CRYPTOGRAPHY AND DIGITAL SIGNATURE SCHEME

The encrypted cloud services are build with Collaborative Cryptography and digital signature techniques. The collaborative cryptography model combines the symmetric and asymmetric cryptography algorithms. The RSA, Elliptic Curve Cryptography (ECC) and Message Digest 6 (MD6) algorithms are applied to improve the security levels. The Key Distribution Center (KDC) is build to manage the key distribution activities with image steganography technique.

The encrypted cloud services are build to share data files with security. Symmetric and asymmetric cryptography techniques are integrated in the system. Data transmission security is guaranteed with digital signature technique. The system is divided into five major modules. They are Cloud Server, Data Owner, Key Distribution Center, Hybrid Cryptography Scheme and Collaborative Cryptography Scheme.

Volume 04, Issue 9, [September– 2017] ISSN (Online):2349–9745; ISSN (Print):2393-8161

The cloud server maintains the shared data files. The shared files are uploaded by the data owners. The key issue operations are managed by the Key Distribution Center (KDC). Symmetric cryptography based security is provided under the Hybrid cryptography scheme. The collaborative cryptography scheme combines the symmetric and asymmetric cryptography techniques.

The cloud server provides storage space for the data owners. Data owners and cloud users details are maintained under the cloud server. The data upload and download operations are managed by the cloud server. Data integrity verification is carried out with the support of the digital signatures maintained under the cloud server.

A. Data Owner

The data owner provides the shared data files for the cloud users. The shared data files are uploaded by the data owners. Data access privileges are managed by the data owners. The shared data values are protected with reference to the selected data security scheme. The Key Distribution Center (KDC) is deployed to manage and distribute the key values for the cloud users. The block, Cryptography scheme and key values are maintained under the images using the Steganography techniques. The key request and response operations are handled by the key distribution center. The key upload, request and response details are maintained under the log files.

The hybrid cryptography scheme is applied to secure the shared data files under the cloud servers. The encryption and decryption operations are carried out using the symmetric cryptography algorithms. The Advanced Encryption Standard (AES), Rivest Cipher 6 (RC6), Byte rotation algorithm (BRA) and Blowfish algorithms are employed for the data security process. The Least Significant Bit (LSB) encoding scheme is used to hide the key and security scheme details into the images. The collaborative cryptography scheme combines the symmetric and asymmetric techniques for the shared data security. The RSA and Elliptic Curve Cryptography (ECC) algorithms are used in the asymmetric cryptography based security process. The public and private key pairs are transferred to the Key Distribution Center (KDC). The data integrity verification is carried out using the Message Digest 6 (MD6) algorithm.

VI. EXPERIMENTAL ANALYSIS

The cloud based data sharing scheme is composed with security and data verification methods.

The shared data values are maintained in encrypted form. Generally one or two cryptography algorithms are used to secure the data values. The Hybrid Cryptography Scheme (HCS) integrates the symmetric key cryptography techniques.

Four symmetric key cryptography algorithms are combined in the Hybrid Cryptography Scheme. The Blowfish, Advanced Encryption Standard (AES), Rivest Cipher (RC6) and Byte Rotation Algorithm (BRA) are used for the same encryption and decryption process. Each block of data is encrypted with separate algorithm. The decryption operations are also carried out with the same manner.

The Collaborative Cryptography Scheme (CCS) combines the symmetric and asymmetric cryptography techniques.

The RSA and Elliptic Curve Cryptography (ECC) algorithm are combined with the hybrid cryptography scheme to build the Collaborative Cryptography Scheme (CCS). The Least Significant Bit (LSB) encoding scheme is used to exchange the key values with in an image. The Message Digest (MD6) algorithm is used for the data verification process. The system is tested with key distribution delay and data access latency parameters.

Volume 04, Issue 9, [September– 2017] ISSN (Online):2349–9745; ISSN (Print):2393-8161

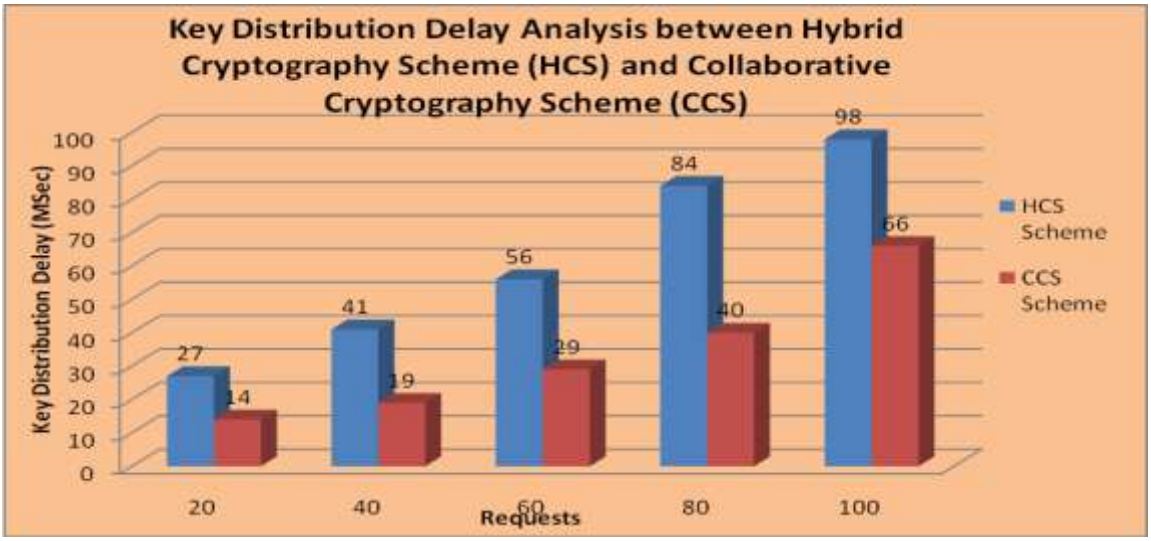

Figure No: 6.1. Key Distribution Delay Analysis between Hybrid Cryptography Scheme (HCS) and Collaborative Cryptography Scheme (CCS)

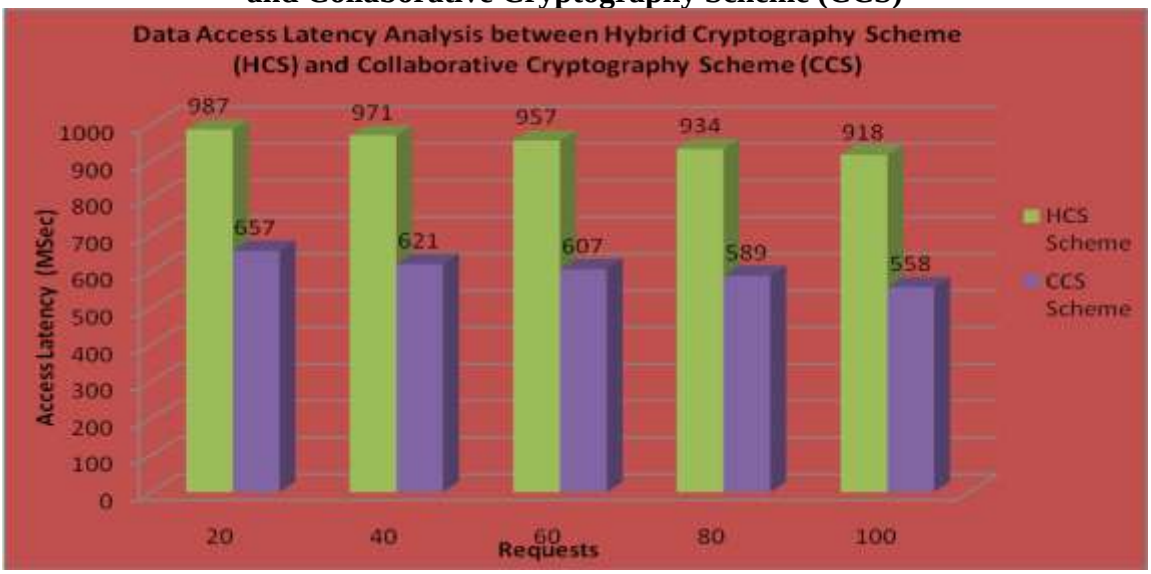

Figure No: 6.2. Data Access Latency Analysis between Hybrid Cryptography Scheme (HCS) and Collaborative Cryptography Scheme (CCS)

The key distribution delay is estimated with key retrieval time period from the key distribution center. The key distribution delay analysis between Hybrid Cryptography Scheme (HCS) and Collaborative Cryptography Scheme (CCS) is shown in figure 6.1.. The Collaborative Cryptography Scheme (CCS) reduces the key distribution delay 40% than the Hybrid Cryptography Scheme (HCS). The data access latency analysis between Hybrid Cryptography Scheme (HCS) and Collaborative Cryptography Scheme (CCS) is shown in figure 6.2.The Collaborative Cryptography Scheme (CCS) reduces the data access latency 35% than the Hybrid Cryptography Scheme (HCS). The data access latency is estimated with data request and response intervals.

VII. CONCLUSION

The encrypted cloud services are build to support secured data sharing operations. The data owner maintains the shared files under the cloud server for the cloud users. The hybrid cryptography scheme combines the symmetric cryptography algorithms with Steganography based key exchange models. The symmetric and asymmetric cryptography algorithms are integrated in the Collaborative Cryptography technique with digital signatures. The collaborative cryptography scheme improves the data security for the encrypted cloud services. The Key Distribution Center (KDC) manages the

Volume 04, Issue 9, [September– 2017] ISSN (Online):2349–9745; ISSN (Print):2393-8161

key transmission based on user requests. Data transmission loses are detected with the support of digital signatures. Data security operations are carried out with multi threaded model.

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "A new general framework for secure public key encryption with keyword search," in Information Security and Privacy - 20th Australasian Conference, ACISP, 2015, pp. 59–76.

[2] H. S. Rhee, J. H. Park,W. Susilo and D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," Journal of Systems and Software, vol. 83, no. 5, 2010.

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

[4] 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, April 2014.

[5] K. Emura, A. Miyaji, M. S. Rahman and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptive security," Security and Communication Networks, vol. 8, no. 8, pp. 1547–1560, 2015.

[6] L. Fang,W. Susilo, C. Ge and J.Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, 2013.

[7] 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 2014.

[8] Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo and Xiaofen Wang, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage", IEEE Transactions On Information Forensics Security, April 2016.

[9] Jasleen K., S.Garg, "Security in Cloud Computing using Hybrid of Algorithms", IJERJS, Volume 3, Issue 5, ISSN 2091-2730,pages 300-305, September-October, 2015.

[10] P. Xu, Q. Wu and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Computers, vol. 62, no. 11, 2013.

