ISSN 2319 - 6629

Volume 8, No.3, April - May 2019

International Journal of Wireless Communications and Networking Technologies

Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt12832019.pdf

https://doi.org/10.30534/ijwcnt/2019/12832019

Encrypted Keyword Search in Cloud Storage

Minnu K Praveen[1], Rittymol Joseph[2], Sajida K N[3] Sornalatha P[4,] Sujitha M[5]

[1]Mangalam College Of Engineering, India, minnukpraveen98@gmail.com
[2]Mangalam College Of Engineering, India, rittymoljoseph960@gmail.com
[3]Mangalam College Of Engineering, India, sajidakn99@gmail.com
[4]Mangalam College Of Engineering, India, latha07111997@gmail.com
[5]Mangalam College of Engineering, India, m.sujitha@mangalam.in

ABSTRACT

Cloud computing is a technology that provides advanced software application and high-end network of server computers. It poses privacy concerns since the server can access the data which is stored in the cloud at any time. In cloud encrypted file search is not possible and it is not secure which is considered as one of the central issues in this area. This paper deals with the technique that uses the cloud to search file in the encrypted form. The relevant of this paper includes, encrypted file search is difficult and not understood by server as well as user. An AES algorithm with ECC scheme and keyword server technique is used to handle this issue efficiently. This technique ensures faster and secure access of files in the cloud.

Key words: AES, ECC, Encryption, Keyword search, Privacy, Security.

1. INTRODUCTION

Cloud storage is a service where data is remotely maintained, managed and backed up. The service allows the users to store files online, so that they can access them from any location via the internet. The goal of cloud computing is to allow users to take benefit from all of the technologies. The main enabling technology for cloud computing is virtualization. Hence the service provider can access the data which is in the cloud, it could accidently delete or alter information. Even though cloud providers can share information with the third parties if needed for any purpose. That is permitted in their privacy policy of cloud, which the user must agree to before they start using cloud services.

The solution of privacy issues in cloud include policy and legislation as well as end users. User can solve this issue by encrypted data that is processed or stored within the cloud. This prevents unauthorized access. Since encrypted file search is difficult and not understood by the server and user, an AES algorithm and keyword search algorithm is used to solve it.

Using our system encrypted file search is possible and it us easily comprehensible by the user. It provides safety and privacy to the file in the cloud by using the algorithm AES and ECC in our system. This system provides extreme resistance towards keyword guessing attacks. Since the key is only known by the keyword server and the cloud. Thus our system provides security. This system encounters the elements of CIA triangle that is confidentiality, integrity and availability to the user. Our framework using three parties: The data owner, trusted cloud server, the data consumer and the keyword server. In the previous model a phrase search technique based on Bloom filters that use a series of n-gram filters to support the functionality. The scheme exhibits a trade-off between storage and false positive rate, and is adaptable to defend against inclusion-relation attacks and design approach based on an application's target false positive rate is also described.

- Software service

The server applications are allowed to run on cloud structure for the usage of customer. The access to these applications can be done from any client.

- Infrastructure service

This service helps the client for all fundamental processing and storage and allows them to install and run arbitrary software.

2. RELATED WORK

Dan Boneh et al proposed a system to overcome the problem of searching on data which is encrypted using a public key. The scheme used on this paper is on public key encryption without revealing the content. A public key encryption standard that is related to Identify Based Encryption (IBE) is showed through this system. But the demerit of this system is that converse of the goal achieved as remained as a problem. The drawback of the scheme is that the public key length grows linearly with the total dictionary size. If an upper-bound on the total number of keyword trapdoors that the user will release to the email gateway, much better using cover-free families and can allow keyword dictionary to be of exponential size. Yanjiang Yang et al. [1][2] proposed a multiuser private keyword search for cloud computing at 2011. This paper introduces searchable encryption is a cryptographic term allowing for private keyword based search over the encrypted database. They proposed various schemes that can accommodate more extensions like ranked keyword search for accessing the database in the encrypted cloud each of the authorized users wants to issue distinct query key to generate valid access queries. Their main objective is that to enable the cloud to process users search queries without learning the keyword containing the queries and the content of the plain text.

M.Zheng and H. Zhou et al. [3] proposed a system on 2013 which offers cipher text search ability method retrieve outscored data from cloud storage.

It also introduces a special adversary to break the provable security reduction scheme. The main reason to introduce this scheme is that the insecurity caused by independency of the indexes which is generated for different keywords. They constructed a clever adversary to break its provable security reduction to make the adversary always successfully picks a random variable generated by any challenge in provable securityreduction.

M.T Goodrich, M. Mitzenmacher, O. Ohrimenko and R. Tamasia et al. these four proposed a system named practical oblivious storage at 2012. Their assumptions model real world cloud storage framework, where trade-off occurs between latency, bandwidth and the size of the client's private memory. B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan et al. proposed a system on private information retrieval in the year of 1995. This discuss about the protection of user privacy from a server was not considered as a feasible solution until the private information retrieval problem and their solution. They mainly focus on the potential applications[4][5].

3. COMMUNICATION FRAMEWORK

We'll describe our framework using three parties. The data owner, trusted cloud server, the data consumer and the keyword server. Advanced encryption standard protocol and elliptic curve cryptography (ECC) curve protocol has been introduced

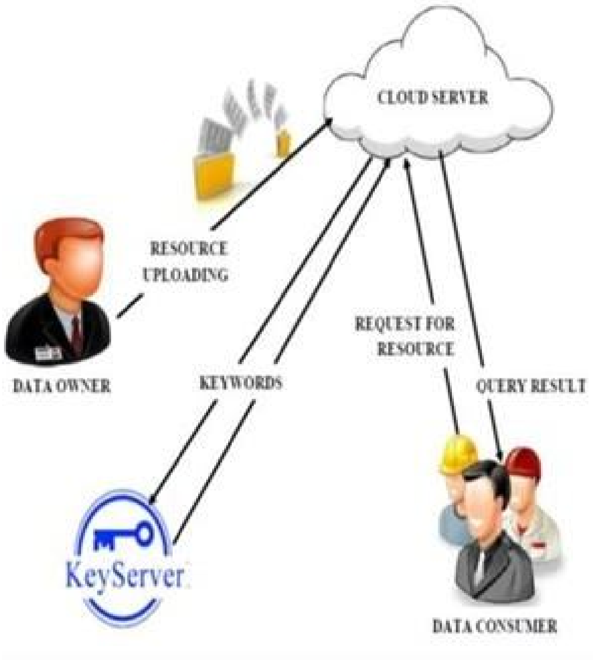

Figure 1: Proposed System

User module: In this module, the resources that are performing are created. The user will be shaped by making the user to fill a registration form. On victorious submission of the registration form, the user can login using the identification. The third party will be the user who can upload the data into system that can be used by the users.

Data owner module: This is the new file creation module, which enable the owner to upload the contents from the cloud server. The document which is to be uploaded will contain various attributes like file name, description about the file and key information's. The content upload will be completed once the data attributes are provided.

Authority grant module: This module aims at creating the authority for users and owners. The users will be provided with access rights like read, write privilege by the owner. Based on the privilege set to the users, the user can access the data. The admin manages the user and the data details.

File Access Module: In this module, we discuss the decryption operation of decrypted data files. A user first obtains with the decrypt algorithm. The rate of decrypting a cipher text varies depending on the key used for decryption. Yet for a given key, the way to assure the coupled access tree may be different. During setup, the data owner wishes to upload documents to the cloud server. For that at the initial stage the user has to be proving that he is an authenticated user to that cloud. The first step to make the user as an authenticated person is to register in the cloud.

The registration of the newly arrived user has to be approved by the admin in order to sign in with the user id and password specified by the user. If not the user won't able to access the page of the cloud. During the time of approval, public and private key along with secrete key will be generated. Since we are using the ECC algorithm in AES scheme, each of the keys generated during the approval of user will be separated as public key, private key and secrete key[8].

The need of applying ECC algorithm is that at the time of uploading of document to the cloud the key server will encrypt the file and then add the secrete key to the encrypted file. After the approval by the admin, the user can login with the id and password the role of third party namely key server is to secure the key. The files that can be uploaded to the cloud are text files and java files. After all these procedures the name and id of user will be saved in database. To add files to the cloud the user need to go for uploading of the file. Initially the users browse the file from the resource and then upload the file to the cloud. In the backdrop of this process the uploaded files will be encrypted with the key is converting to a cipher text. [9][10].Along with the cipher text the key that is generated at the time of user registration is added to it. The key s unknown to the user only the server and cloud will be aware of it. The encrypted file plus the key will be saved to the cloud and key itself will be stored in the key server. The key word server and the cloud will work concurrently.

Consider an attacker who is attempting to lookup the file from the cloud using the key. This key is not access able by the attacker because the key is not known by the consumer or the owner. Because of the concurrent access of server and cloud. It is not revealed to no one else. A consumer can retrieve the file by using the query and as a result the required file is viewed to them.

Private Key: It is the form of encryption; a single private key can encrypt and decrypt information. The private key is a fast process; hence it uses a single key. In business, the private key is needed to secure the information confidential such as it includes the data of the customer, intellectual property, research and development. In this private key encryption, it protecting one key and it creates a key management issue because everyone is using private keys. It may be stolen or leaked. So, the key management requires changing in the encryption key often and prevention of risks and it should be appropriately distributing the key[13].

Public Key: A public key is a large geometric value that is used to encrypt data. The key can be created by a software program, but more often, it is provided by a trusted, selected specialist made available to everyone through a publicly accessible depository or directory. The public key can be openly distributed without conceding security[11][12].

Secret Key: It is also called symmetric key because here same key is used for encrypt and decrypt. The major issue with secret key is the logistic problem i.e.; how to get a key from one party to the other without allowing access to an attacker.

Encryption: Encryption is the process of encoding a text message so that only authorized parties' can accessed the data and unauthorized parties cannot access. In an encryption method plain text is encrypted using an encryption algorithm. As a result, a cipher text is generated that can be read only if decrypted. For a high encryption scheme computational resources and skills are required. If the client is an authorized recipient decryption can be done easily. Encryption is most effective way to achieve datasecurity[7].

Decryption: It is the process of transmuting data that has been rendered unreadable through encrypt back to its unencrypted form. The system abstracts and converts the garbled data and translates it to the reader but also by the system. The most important reason for implementing an encryption-decryption system is to ensure privacy. It guarantees the subject to surting and access from unauthorized entities or groups. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email message, text files, images, user data and directories. It can undertake physically or mechanically.

AES (Advanced Encryption Standard): AES is a symmetric block cipher, to protect classified information and is implemented in software and hardware throughout the world to encrypted sensitive data. Easy to implement in hardware and software, as well as in restricted environments and offer good defenses against various attack technique.

Features of AES;

- Security: Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, through security strength was to be considered the most important factor in the competition.
- Cost: Intended to be released under a global, nonexclusive and royalty free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- Implementation: Algorithm and implementation characteristics to be evaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software and overall, relative simplicity of implementation.

ECC (Elliptic Curve Cryptography): Elliptic curve cryptography is relevant for key agreement, digital signature for factoring integer, principally providing and in public key cryptography. These systems provide comparatively small block sizes, high speed software and hardware performance, and after the highest strength per key bit of any known public key scheme. They can be used for encryption by computing the key agreement with a symmetric encryption system.

CIA Triangle: CIA is also called CIA triad, designed to guide for information security sometimes it referred as AIC. Because to avoid confusion with central intelligence agency.

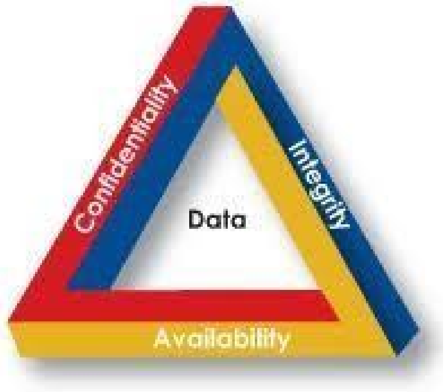

Figure 2: CIA Triangle

- Confidentiality.

Confidentiality involves a set of rules or a promise usually executed through privacy agreements that limits access limitations on certain file types of information's. it is the skill to hide information from those people with unsanctioned to it. It unevenly corresponds to privacy and data encryption is a common method of ensuring confidentiality[6].

- Integrity.

Data integrity preservation is an information security. Integrity is a chief module of information assurance because the users must be able to trust information. Data integrity means data should be kept from unauthorized alteration in the cloud computing. Any adjustment to the data should be detected. Computation integrity means that program execution should be expected and be kept away from malware.

- Availability.

Availability is best ensures maintaining all hardware, performing hardware maintenance instantaneously. When needed and maintaining a accurately functioning operating system environment that is free from software conflicts. It is also vital to keep present with all essential system upgrades.

4. EXPERIMENTAL RESULT

Encrypted file search is the main drawback noticed in the former system. Using our system encrypted file search is possible and it us easily comprehensible by the user. It provides safety and privacy to the file in the cloud by using the algorithm AES and ECC in our system. This system provides extreme resistance towards keyword guessing attacks. Since the key is only known by the keyword server and the cloud.

The key is not in the storage of cloud hence the cloud cannot access the data and the key is not in the information of the user so that the attacker won't able to recover the key from the user side. Thus our system provides security. This system meets the content of CIA triangle that is confidentiality, integrity and availability to theuser.

5.CONCLUSION

By the system we met the confidentiality, integrity, availability of data; we make sure that the system is highly safe and sound against keyword guessing attack and other type of vulnerable attacks. In the view of the fact that it provides encrypted keyword search of file in cloud. This system exceedingly sheltered against malware and worms.

.REFERENCES

[1] PranitR.Thite, Ganesh M.Suryawanshi, Rajesh Mengale, Prof. A.M.Ingole “Data Search In Cloud Using The Encrypted Keywords” *International Research Journal of Engineering and Technology (IRJET)* e-ISSN: 2395-0056 Volume: 04 Issue: 11 Nov -2017.

[2]Birendra Goswami, Dr.S.N.Singh “Enhancing Security

[3]in Cloud computing using Public Key Cryptography with Matrices” *International Journal of Engineering Research and Applications (IJERA*) ISSN: 2248-9622Vol. 2, Issue 4, July-August 2012, pp.339-344.

[3]N.Meenakshi and G.Sasikala“Cloud Storage Auditing with Key Generation Using Blowfish Algorithm”*International Journal of Computing Academic Research (IJCAR*) ISSN 2305-9184, Volume 5, Number 1 (February 2016), pp.63-71. https://doi.org/10.1080/0449010X.2016.1270517

[4] Anuradha N. M “Secure and Efficient Data Retrieval in Cloud Computing” *International Journal of Engineering Research & Technology (IJERT)* ISSN: 2278-0181 Vol. 4 Issue 04, April-2015. https://doi.org/10.17577/IJERTV4IS041017

[5]Raghavendra S, Chitra S Reddy, Geeta C M, Rajkumar Buyya, Venugopal K R, S SIyengar, L M Patnaik “Survey on Data Storage and Retrieval Techniques over Encrypted Cloud Data” *International Journal of Computer Science and Information Security (IJCSIS),* Vol. 14, No. 9, September 2016.

[6] M.Gowthame“Phrase Based Search Technique for Secure Storage and Access of Confidential Documents”*International Journal of Pure and Applied Mathematics*, Volume 119 No. 15 2018, 275-282.

[7]Pavan Kumar Kandukuri,G. Vishnu Murthy “A Survey on Phrase Search over Encrypted Cloud Storage with Multiple Data Owners”*International Journal of Engineering Research in Computer Science and Engineering (IJERCSE*) Vol 5, Issue 4, April 2018.

[8] Dawn Xiaodong Song, David Wagner Adrian Perris“Practical Techniques for Searches on Encrypted Data” University *of California, Berkele*, 2008

[9]Dan Boneh, Giovanni Di Crescenzo“Public Key Encryption with keyword Search*” Stanford University*, 2001.

[10]Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou “Secure Ranked Keyword Search over Encrypted Cloud Data” 2010 *International Conference on Distributed Computing Systems.* https://doi.org/10.1109/ICDCS.2010.34

[11]D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in *proceedings of Euro crypt*, 2004, pp. 506–522. https://doi.org/10.1007/978-3-540-24676-3_30

[12]M. Zheng and H. Zhou, “An efficient attack on a fuzzy keyword search scheme over encrypted data,”in *International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing*, 2013, pp. 1647-1651 https://doi.org/10.1109/HPCC.and.EUC.2013.232

[13]Y. Yang, H. Lu, and J. Weng, “Multi-user private keyword search for cloud computing,” in *IEEE Third International Conference on Cloud Computing Technology and Science*, 2011, pp. 264–271. https://doi.org/10.1109/CloudCom.2011.43