RESEARCH ARTICLE OPEN ACCESS

Server-Designation Preventive Scheme for Public key Encryption with Keyword Search Cryptographic Primordial

[1]A.Senthil Kumar, [2]S.Vimal

[1]Asst.professor, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

--**********************---------------------------

Abstract:

In this work, we travel around the security of an exceptional cryptographic primordial, in meticulous Public Key Encryption with Keyword Search (PEKS) which is outstandingly helpful in numerous utilizations of scattered storage. Horrendously, it has been verified that the customary PEKS classification experiences an incontrovertible instability called inside Keyword Guessing Attack (KGA) propelled by the spiteful server. Cloud storages in cloud data centres can be used for enterprises and persons to store and access their data remotely anywhere anytime without any further load. By data outsourcing, users can be relieved from the encumber of local data storage and protection. we consider refuge of the well-known cryptographic primitive, namely, public key file encryption with keyword search (PEKS) that is very helpful in lots of applying cloud storage. Regrettably, it's been proven the traditional PEKS framework is affected with a natural insecurity known as inside keyword guessing attack (KGA) launched through the malicious server. To deal with this security vulnerability, we advise a brand new PEKS framework named dual-server PEKS (DS-PEKS). Then we show a normal construction of secure DS-PEKS from LH-SPHF. We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we provide an efficient instantiation of the general framework from a DDH-based LH-SPHF and show that it can achieve the strong security against inside KGA.

Keywords —**Secure Cloud Storage; Encryption; Cloud Computing, Security, Encryption Techniques**

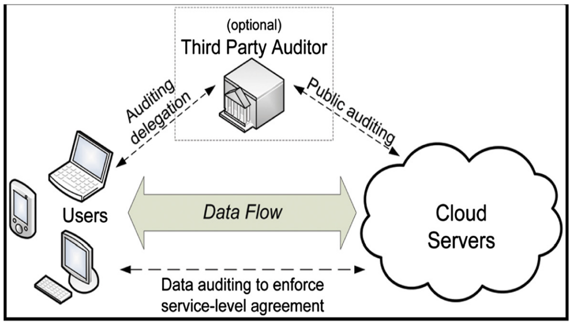
--**********************---------------------------

I. INTRODUCTION

The typical solutions may be the searchable file encryption which enables the consumer to retrieve the encrypted documents which contain the consumer-specified keywords, where because of the keyword trapdoor, the server will find the information needed through the user without understanding. Searchable file encryption could be recognized either in symmetric or uneven files encryption setting. Public key encryption with keyword search(PEKS) is a notion of dealing with obtaining encrypted data from the servers with regard to cloud storages. PEKS enables a sender stores encrypted sensitive data with searchable cipher texts into a server. A receiver who wants to obtain the sender's sensitive data should provide a keyword trapdoor to the server. After testing the validness of the keyword trapdoor with searchable cipher texts, the server will send the encrypted sensitive data to the receiver.

Decoded client information put away at the remote cloud server can be defenseless against outer assaults started by unapproved outcasts and inside assaults started by the dishonest cloud service provider (CSPs) organizations. There are a few reports that affirm information breaks identified with cloud servers, because of malignant assault, burglary or inward mistakes. This raises sympathy information may contain extremely delicate individual association/data.

Distributed cloud storage outsourcing has turned into a prominent application for undertakings and associations to lessen the weight of keeping up enormous information lately. No withstanding, in all actuality, end clients may not by any means believe the cloud capacity servers and may want to scramble their information some time recently transferring them to the cloud server with a specific end goal to secure the information protection. This normally makes the information usage more troublesome than he conventional storage where information is kept in the nonappearance of encryption. One of the average arrangements is the searchable encryption which permits the client to recover.



Several methods have been put forward to tackle the issue of privacy preserving. Some researchers have been conducted with the aid of third party auditor (TPA) to verify the data stored in the cloud and be sure that it is not tampered. The TPA can perform the auditing on behalf of a user and provide the audit report to the user. This technique is also useful for cloud service providers (CSP) to maintain its reputation by getting higher reliability, consistency, and data integrity ratings or certificates from TPA to improve their business on commercial point of view. However, the major problem that arises with this approach is that the TPA was leased by the provider, and after a time, the cloud service provider may contract with the TPA to conceal the loss of data from the user to prevent the defamation. As a result, the correctness of the data in the cloud storage is being put at risk.

1.1.Traditional PEKS

Taking after Boneh et al's. Fundamental work, Abdalla et al. formalized unknown IBE (AIBE) and exhibited a nonexclusive development of searchable encryption from AIBE. They likewise demonstrated to exchange a progressive IBE (HIBE) conspire into an open key encryption with brief catchphrase seek (PETKS) where the trapdoor is as it were legitimate in a particular time interim. Waters demonstrated that the PEKS plans in light of bilinear guide could be connected to assemble scrambled and searchable reviewing logs.

1.2.Secure Channel Free PEKS

The first PEKS plot requires a protected channel to transmit the trapdoors. To beat this confinement, Baek et al. Proposed another PEKS plot without requiring a protected channel, which is alluded to as a protected without channel PEKS (SCF-PEKS). The thought is to include the server's private key combine into a PEKS framework. The watchword cipher text and trapdoor are produced utilizing the server's open key and thus just the server (assigned analyzer) can play out the hunt.

1.3.Keyword Guessing Attack

Bynum et al. presented the disconnected catchphrase speculating assault against PEKS as watchwords are looked over a much littler space than passwords what's more, clients as a rule utilize understood catchphrases for looking archives. They likewise called attention to that the plan proposed in Boneh et al. was defenseless to watchword speculating assault. Enlivened by the work of Byun et al. Yau et al. exhibited that outside foes that catch the trapdoors sent in an open channel can uncover the encoded watchwords through disconnected Key guessing attack and they likewise flaunted line watchword speculating assaults against the (SCF-)PEKS conspires .The principal PEKS conspire secure against outside Key guessing attack was proposed by Rhee et al. . In , the idea of trapdoor vagary was proposed and the creators appeared that trapdoor vagary is an adequate condition for avoiding outside watchword speculating assaults.

II. SECURITY MODELS

Subsection, we formalise the following security models for a DS-PEKS scheme against the adversarial front and back servers, respectively. One should note that both the front server and the back server here are supposed to be "honest but curious" and will not collude with each other. More precisely, both the servers perform the testing strictly following the scheme procedures but may be curious about the underlying keyword. We should note that the following security models also imply the security guarantees against the outside adversaries which have less capability compared to the servers.

2.1.Adversarial Front Server.

we define the security against an adversarial front server. We introduce two games, namely semantic-security against chosen keyword attack and indistinguishability against keyword guessing attack.

III. CLOUD COMPUTING

The simplified definition for Cloud Computing is to move computing from the PC to a central data over the Internet. Also, Cloud Computing is isolated a lot of complexity that associated with cost, components management, and software and make it easy service via the Internet. As the cloud computing consists of modern technological concepts such as Service Oriented Architecture (SOA), Web Services (WS), and communication infrastructure.

- ***Scalability***: Cloud computing has the flexibility to expand in terms of users or storage,
- ***Flexibility***: Cloud computing provides users flexibility in terms of increasing or decreasing the resources used,
- ***Pay as you used***: In cloud computing cost is calculated based on its use, and
- ***Self-identify resources***: In cloud computing subscribers can determine the appropriate capacity for them related to processing, software, and storage.

IV. CLIENT/SERVER ARCHITECTURE

The system consist of an admin. The admin creates the actors and provide the rights to the actors. The actors that are involved in the hospital environment are doctor, patients, medical shop, insurance agent. Doctor uploads the treatment history to the centralized server in the encrypted form which uses the attribute based encryption. The patient and doctor have the right to access the full data according to the role provided to the actors, during the decryption they fetch the data.

V. CONCLUSION

In this paper, a new framework, named Dual-Server Public Key Encryption with Keyword Search, that can prevent the inside keyword guessing attack which is an inherent vulnerability of the traditional PEKS framework. An Attribute Based Encryption along with Dual key encryption is proposed to increase the security of private health record system stored in the cloud. This solution ensures discretion of the health records and fortification from unconstitutional users. It also keeps the login details of the actors and provides faster accessibility to the actors as a unique key is used. Owing to the shown weaknesses, we enhanced the existing security models for trapdoor indistinguishability by defining two new security models. We also proposed a new framework.

VI.REFERENCE

[1] Abdalla, M. et al.: 'Searchable encryption revisited: consistency properties, relation to
anonymous ibe, and extensions'. J. Cryptol., 21, 2008. pp. 350-391.

[2] Baek, J., Safavi-Naini, R., Susilo, W.: 'Public Key Encryption with Keyword Search
Revisited'. ICCSA'08. 5072(2008). pp.1249-1259.

[3] K. Emura, A. Miyaji, M. S. Rahman, and K.Omote, "Generic constructions of securechannel free searchable encryption with adaptive security," Secur. Commun. Netw., vol. 8, no. 8, pp. 1547–1560, 2015.

[4] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding. Cirencester, U.K.: Springer, 2001, pp. 360–363.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT, 2004, pp. 506–522.

[6] S Bhagyashri, YB Gurave, A survey on privacy preserving techniques for secure cloud storage. International Journal of Computer Science and Mobile Computing (IJCSMC) 3(2), 675–680 (2014).

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in NDSS, 2004.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in CRYPTO, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based on k-resilient IBE," in Computational Science and Its Applications -ICCSA, 2006, pp. 298–308.

[10] P. Xu, H. Jin, 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, pp. 2266– 2277, 2013.