IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003198

A Certain Build up Key PolicyAttribute-Based Temporary Keyword Search Strategy inthe Cloud

Mr.G.Yuvaraj[1], Akuluru Harshitha[2], Hasita.K[3]

Assistant Professor Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

U.G Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: Cloud computing (ABKS) is widely used for secure cloud storage. In the existing system the algorithm used is key-policy attribute-based temporary keyword search (KP-ABTKS) where the private key is the access system that controls user's search power in which the data security cannot be ensured. In the proposed system cipher policy attribute-based encryption (CP-ABE) is used where the data is stored in a cipher text format undergoing double encryption to overcome the drawback in the existing system. The CP-ABE comes under the Lightweight Data Sharing Scheme (LDSS). As an important computer application, storage can reduce the price and distributing data in a cloud. For example, email data, and financial documents stored in Cloud may be compromised by an attack. One of the best ways to protect sensitive data is by encrypting it and entering text into the cloud. But traditional Cryptographic schemes prevent users from recovering their data. In the PEKS program, the database encrypts each file and stores the encryption script in the cloud. Cloud server associated with the signal with a keyword can retrieve data by testing whether the search token and the cipher text correspond to the same keyword. As an important type of cloud computing, cloud computing (ABKS) is widely used for secure cloud storage.

KEYWORDS: Cipher text , Cipher policy-Attribute Based Encryption , Lightweight Data Sharing Scheme.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide accessto advanced software applications and high-end networks of server computers.

Characteristics and Services Models of Cloud:

In figure 1 The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi- tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003198

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quicklyscale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

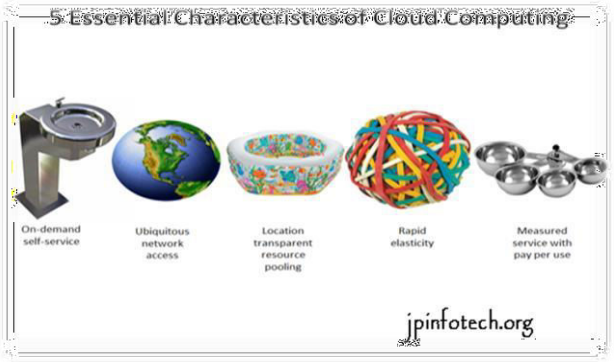

Figure 1 Characteristics of Cloud Computing

II. LITERATURE SURVEY

[1] In the year 2018 Javad Mohajeri has proposed for Public key encryption with keyword search (PEKS) is a well-known cryptographic primitive for secure searchable data encryption in cloud storage. Unfortunately, it is inherently subject to the (inside) offline keyword guessing attack (KGA), which is against the data privacy of users. Existing countermeasures for dealing with this security issue mainly suffer from low efficiency and are impractical for real applications. In this paper, we provide a practical and applicable treatment on this security vulnerability by formalizing a new PEKS system named server-aided public key encryption with keyword search (SA-PEKS). In SA-PEKS, to generate the keyword ciphertext/trapdoor, the user needs to query a semitrusted third-party called keyword server (KS) by running an authentication protocol, and hence, security against the offline KGA can be obtained. We then introduce a universal transformation from any PEKS scheme to a secure SA-PEKS scheme using the deterministic blind signature. To illustrate its feasibility, we present the first instantiation of SA-PEKS scheme by utilizing the Full Domain Hash RSA signature and the PEKS scheme proposed by Boneh et al. in Eurocrypt 2004. Finally, we describe how to securely implement the client-KS protocol with a rate-limiting mechanism against online KGA and evaluate the performance of our solutions in experiments.

[2] In the year 2019 Chengyu hu has proposed Public-key encryption with keyword search (PEKS) enables users to search on encrypted data, which is applicable to the scenario of sharing data in the cloud storage. In this paper,we focus on how to construct a PEKS scheme via obfuscation. Our basic scheme is built on the differing-inputs obfuscation (diO) and can be considered as an initial attempt to apply diO in the PEKS field. The scheme supports searching on encrypted data by providing to the cloud server an obfuscated simple ‘‘decrypt-then-compare’’ circuit with the secret key and the queried keyword hardwired in it. More interestingly, the scheme can be simplyimproved to resist off-line keyword guessing attacks (KGAs) as the standard PEKS scheme rather than a designated tester one. For complex search conditions, our scheme can be easily extended to multiple functionalities, such as conjunctive and fuzzy keyword search. Furthermore, it can be extended to the PEKS scheme in the multi-user setting.

[3] In the year 2015 Kaitai lang has proposed the growth of electronic personal data leads to a trend that data owners prefer to remotely outsource their data to clouds for the enjoyment of the high-quality retrieval and storage service without worrying the burden of local data management and maintenance. However, secure share and search for the outsourced data is a formidable task, which may easily incur the leakage of sensitive personal information. Efficient data sharing and searching with security is of critical importance. This paper, for the first time, proposes a searchable attribute-based proxy reencryption system. When compared with the existing systemsonly supporting either searchable

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003198

attribute-based functionality or attribute-based proxy reencryption, our new primitive supports both abilities and provides flexible keyword update service. In particular, the system enables adata owner to efficiently share his data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The new mechanism is applicable to many real-world applications, such as electronic health record systems. It is also proved chosen ciphertext secure in the random oracle model.

[4] In the year 2017 Chen, R.,has proposed the Public key encryption with keyword search (PEKS) is a well- known cryptographic primitive for secure searchable data encryption in cloud storage. Unfortunately, it is inherently subject to the (inside) offline keyword guessing attack (KGA), which is against the data privacy of users. Existing countermeasures for dealing with this security issue mainly suffer from low efficiency and are impractical for real applications. In this paper, we provide a practical and applicable treatment on this security vulnerability by formalizing a new PEKS system named server-aided public key encryption with keyword search (SA-PEKS). In SA-PEKS, to generate the keyword ciphertext/trapdoor, the user needs to query a semitrusted third-party called keyword server (KS) by running an authentication protocol, and hence, security against the offline KGA can be obtained. We then introduce a universal transformation from any PEKS scheme to a secure SA-PEKS scheme using the deterministic blind signature. To illustrate its feasibility, we present the first instantiation of SA-PEKS scheme by utilizing the Full Domain Hash RSA signature and the PEKS scheme proposed by Boneh et al. in Eurocrypt 2004. Finally, we describe how to securely implement the client-KS protocol with a rate-limiting mechanism against online KGA and evaluate the performance of our solutions in experiments.

III. EXISTING SYSTEM

In general, we can divide these approaches into four categories: simple ciphertext access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-basedencryption (ABE). All these proposals are designed for non-mobile cloud environment. Tysowski et al. considereda specific cloud computing environment where data are accessed by resource-constrained mobile devices, and proposed novel modifications to ABE, which assigned the higher computational overhead of cryptographic operations to the cloud provider and lowered the total communication cost for the mobile user.

IV. LIMITATIONS

Data privacy of the personal sensitive data is a big concern for many data owners. The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient. They cannot meet all the requirements of data owners. They consume large amount of storage and computation resources, which are not available for mobile devices. Current solutions don't solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobiledevices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud.

V. PROPOSED SYSTEM

We propose a Lightweight Data Sharing Scheme (LDSS) for cloud computing environment. We design an algorithm called CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext. We use proxy servers for encryption and decryption operations.

Figure 2 describes the architecture diagram of the proposed system and list the overall modules of the proposed system

System Framework

The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model. In these applications, data owners can upload their documents and other files to the cloud and share these data with other data users they like to share.CSPs also provide data management functionality for data owners.We propose LDSS, a framework of lightweight data sharing scheme in mobile cloud.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003198

Data Owner

When the data owner registers on TA, TA runs the algorithm Setup() to generate a public key PK and a master key MK.PK is sent to DO while MK is kept on TA itself. DO uploads data to the mobile cloud and share it withfriends.DO sends data to the cloud. The DO defines access control policy in the form of access control tree.

Data User

DU logins onto the system and sends, an authorization request to TA. TA accepts the authorization request and checks the request and a generate attribute keys (SK)for DU.DU receives the cipher text, which includes cipher text of data files and cipher text of the symmetric key. DU decrypt the cipher text of the symmetric key with the assistance of (Decryption service provider) DSP.

Trusted Authority

DU logins onto the system and sends, an authorization request to TA. TA accepts the authorization request and checks the request and a generate attribute keys (SK)for DU.DU receives the cipher text, which includes cipher text of data files and cipher text of the symmetric key. DU decrypt the cipher text of the symmetric key with the assistance of (Decryption service provider) DSP.

Cloud Service Provider

CSP stores the data for DO.It faithfully executes the operations requested by DO. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses the request.CSP manages the Uploaded Files.

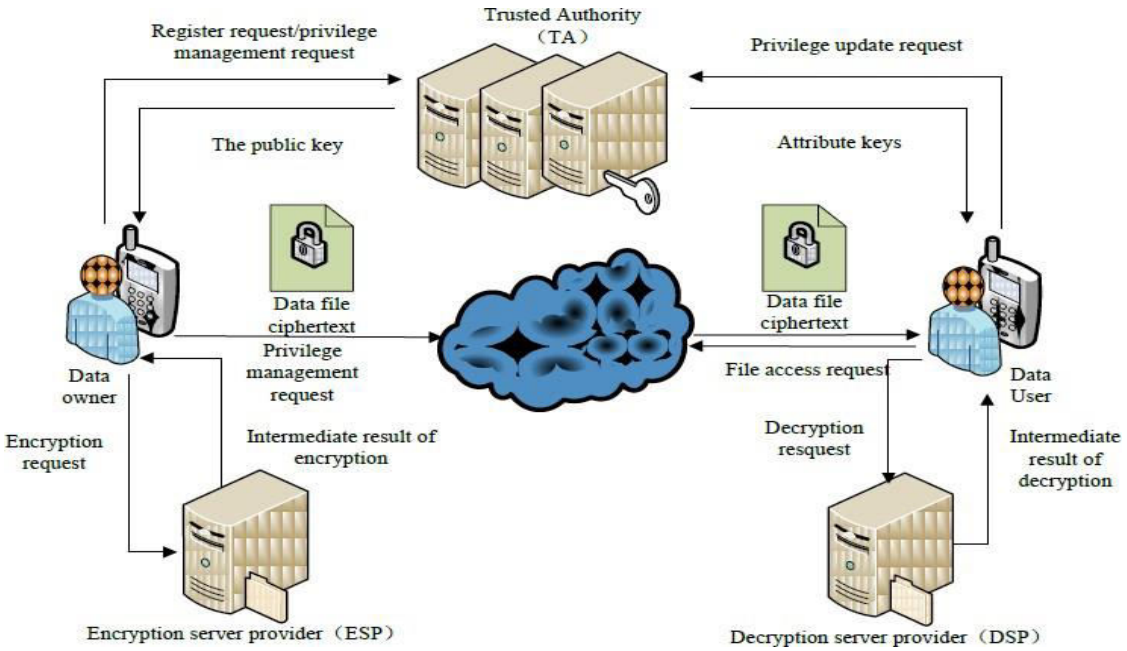

Figure 2.Architecture diagram

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003198

VI. ADVANTAGES

The results also show that LDSS has better performance compared to the existing ABE based access control schemes over cipher text.Multiple revocation operations are merged into one, reducing the overall overhead.The proposed scheme achieves both fine-grained search control and temporary keyword search simultaneously. In addition, the performance evaluation indicates that our scheme is practical.

VII. EXPERIMENTAL RESULTS

Figure 3 shows the result of login pages and storing the data in a secured manner using cloud computing based onCipher policy Attribute-based encryption algorithm. Figure 4 shows the key generated by the trusted authority to access the file.

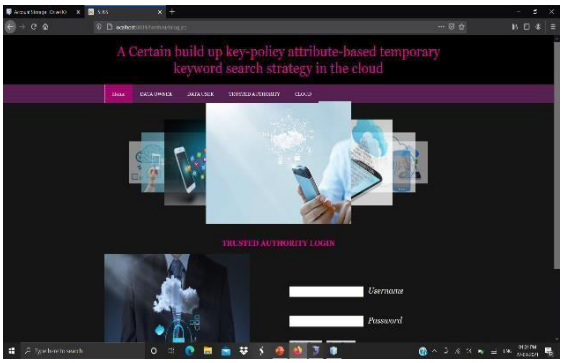

Figure 3 Trusted Authority login

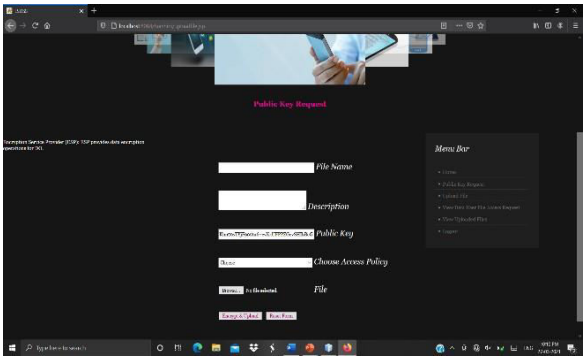

Figure 4 Public Key

VIII. CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE).However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue.It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers,thus it can solve the secure data sharing problem in mobile cloud.The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

REFERENCES

[1] M. H. Ameri, M. Delavar, J. Mohajeri, and M. Salmasizadeh, "A keypolicy attribute-based temporary keyword search scheme for secure cloud storage," IEEE Transactions on Cloud Computing, pp. 1–1, 2018.
[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in International conference on the theory and applications of cryptographic techniques. Springer, 2004,pp. 506–522.
[3] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014,pp. 522–530.
[4] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 226–234.
[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Annual International Conference on the Theoryand Applications of Cryptographic Techniques. Springer, 2005, pp. 457–473.
[6] Y. Yu, J. Ni, H. Yang, Y. Mu, and W. Susilo, "Efficient public key encryption with revocable keyword search," Security

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003198

and Communication Networks, Vol. 7, no. 2, pp. 466–472, 2014.
[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[8] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, Vol. 2003, pp. 216, 2003.
[9] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Transactions on Information Forensics and Security, Vol. 11,no. 12, pp. 2706–2716, 2016.
[10] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, Vol. 27, no. 2, pp. 340– 352, 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details