VERIFIABLE AND MULTI-KEYWORD SEARCHABLE ATTRIBUTE-BASED ENCRYPTION SCHEME FOR CLOUD STORAGE

Dr.E.Punarselvam[1],Mr.M.Dhamodaran[2], M.Saravanan[3], S.Sasidharan[3], S.Sreedhar[3], K.Vignesh[3]

E-Mail:1.hod.it@mec.edu.in,punarselvam83@gmail.com,2.dhamodaran.m.it@mec.edu.in

1. Head of the department, 2.Assistant Professor, 3.Final Year student
Department of Information Technology, Muthayammal Engineering College, Tamilnadu.

ABSTRACT

The success of the cloud computing paradigm is due to its on-demand, self-service, and pay-by-use nature. Public key encryption with keyword search applies only to the certain circumstances that keyword cipher text can only be retrieved by a specific user and only supports single-keyword matching. In the existing searchable encryption schemes, either the communication mode is one-to-one, or only single-keyword search is supported. This paper proposes a searchable encryption that is based on attributes and supports multi-keyword search. Searchable encryption is a primitive, which not only protects data privacy of data owners but also enables data users to search over the encrypted data. Most existing searchable encryption schemes are in the single-user setting. There are only few schemes in the multiple data users setting, i.e., encrypted data sharing. Among these schemes, most of the early techniques depend on a trusted third party with interactive search protocols or need cumbersome key management. To remedy the defects, the most recent approaches borrow ideas from attribute-based encryption to enable attribute-based keyword search (ABKS).

KEYWORDS: Public Key, Encryption Schemes, ABKS,Data Sharing.

1. INTRODUCTION

With the development of cloud computing, many of information can be shared through computer networks. The cloud server (CS) can provide users with a variety of services, such as outsourcing commission calculations and data storage. Users can store their large amounts of data to the CS and share data with other users. For the purpose of the security of storage data and user's privacy, data is usually stored in encrypted form in CS. However, under this environment users will encounter a difficulty problem of how to search keyword in cipher text. Searchable Encryption (SE) is a cryptographic technology that has been developed for many years, which supports users' keyword search in cipher text. In the meanwhile, it can save a lot of network and computational overhead for user, and take advantage of the huge computing power of CS. The SE technology mainly solves the problem of how to use the server to complete the search for interesting keywords when the data is encrypted and stored in CS, but CS is not completely trusted. How to improve the efficiency of keyword search while reducing local computing load is still a problem to be solved. Most of existing schemes support single-keyword search. Single-keyword search waste network bandwidth and computing resources, as this search method returns a large number of results, this means that the search result is not accurate. That is, when a data user uses multi- keyword search, the cloud sever will return relatively few number of files containing these multikeyword, thus the search result is much more accurate than when a data user uses one keyword search. In order to solve this problem, multi-keyword search is proposed. Most of existing attribute-based encryption (ABE) schemes have high computational costs at user client. These problems greatly limit the applications of ABE schemes in practice.

Specifically, our scheme supports three functions: (1) multiple keyword searches; (2) full outsourcing; (3) verifiability of outsourced private keys. Therefore, by changing some specific constructions of the algorithm, the three main advantages of our scheme can be extended to the general attribute-based encryption scheme (such as the encryption scheme without considering the local computing burden, or the encryption scheme lacking the cipher text search). Achieve the ability to reduce local computing storage and accurately search cipher text.

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 access to advanced software applications and high-end networks of server computers.

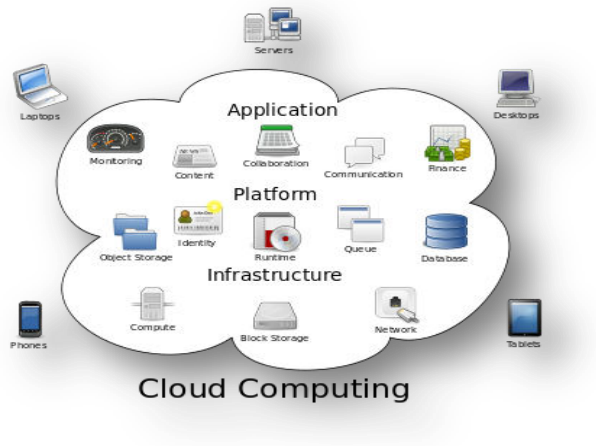

Figure 1 Structure of cloud computing

Cloud Computing Works

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

2.CHARACTERISTICSAND SERVICES MODELS

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.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale 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.

3. SERVICES MODELS

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If

she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

4.EXISTING SYSTEM

Public Key Encryption (PKE), the privacy required by means of the patients could stand ensured. Up in conformity with now, much cryptographic encryptions strategies bear been proposed after fulfill the necessities about privacy- retaining in tremendous records storage. However, near encryption strategies such as like the masses key encryption are no longer anonymous, i.e., salvo the adversaries reap the cipher texts, that may effortlessly be aware of the owner regarding the cipher text as like nicely as whoever desire get hold of the cipher text. The PKE can't acquire the anonymity concerning the customer's ship then get hold of the cipher text, hence private facts may additionally remain leaked. If an opposite is capable after achieve the cipher text, that perform recognize whose solution the cipher textual content is encrypted under, accordingly understanding the proprietor of the cipher text.

4.1 DISADVANTAGES

- Encryption strategies such so the populace authorization encryption are not anonymous.
- The adversaries reap the cipher texts, he do without problems are aware of the proprietor regarding the cipher text so nicely as whomever intention gets hold of the cipher text.
- They might also will according part records only including receivers who have certain attributes. Data carriers then receivers hold to affirm the truth concerning each lousy according to redact sure that data or the identity won't keep leaked out.
- The attributes additionally need according to keep protected.

5. PROPOSED SYSTEM

This proposes a searchable encryption that is based on attributes and supports multi-keyword search. Searchable encryption is a primitive, which not only protects data privacy of data owners but also enables data users to search over the encrypted data. Most existing searchable encryption schemes are in the single-user setting. There are only few schemes in the multiple data users setting, i.e., encrypted data sharing. Among these schemes, most of

the early techniques depend on a trusted third party with interactive search protocols or need cumbersome key management. To remedy the defects, the most recent approaches borrow ideas from attribute-based encryption to enable attribute-based keyword search (ABKS).

5.1ADVANTAGES

- First proposed the notion about the privacy about the keys is high secure.
- The most recent approaches borrow ideas from attribute-based encryption to enable attribute-based keyword search (ABKS).
- Achieving attributes authentication earlier than re-encryption, or ensuring the protection over the attributes and data.
- Receivers whoever are certified in imitation of know the information do use their keys in conformity with decrypt the cipher text, however others cannot, consequently data providers' privations be able stand protected.
- To perfect the current PRE system considered the scenario to that amount information companies may additionally need the records to stay conditionally shared. That capability receiver just gains a quantity on the facts as an alternative on the whole. Such deference is greater close in imitation of the reality.

6.METHODOLOGYS

- Attribute Authority
- Cloud Server
- Key Generation Server
- Data Owner
- Data User

Attribute Authority (AA)

The AA is attribute authority, which is responsible for system's initial establishment and the local secret key generation of data user. Simultaneously, it distributes corresponding secret key according to attribute set for data user. When an attribute is revoked, AA generates an update key and completes partial secret key update.

Cloud Server (CS)

The CS stores cipher text which containing encrypted files and keyword indexes generated by data owners. Afterwards, when a data user tends to search cipher text, CS completes a matching of data user's token and keyword index. If matching

succeeds, it sends cipher text to data user. Additionally, in attribute revocation phase, CS is responsible for updating cipher text.

Key Generation Server (KGS)

The KGS generates data user's partial secret key, namely outsourced secret key, which effectively reduces the computational burden of AA. Besides, KGS is responsible for completing the update of outsourced secret key when attribute revocation happens.

Data Owner (DO)

The DO encrypts keyword set and file to be shared, uploads cipher text to cloud server. Only attribute set of data user who wants to access data satisfies access structure in cipher text. The encrypted data will be shared with data user. To be specific, the encryption operation to be completed by DO includes: the keyword index generation, the file encryption, and the encryption of key for encrypted file, hence cipher text consists of three parts.

Data User (DU)

When data user's attribute set satisfies access structure in cipher text, then data user DU is able to access encrypted data and recover original plaintext. Specifically, DU generates desired keyword token and sends to cloud server CS, the CS makes a matching between search token and keyword index, if matching succeeds, DU can download corresponding cipher text. In other words, DU is responsible for generating keyword token which he is interested in and decrypting cipher text.

7. CONCLUSION

In this article we proposed VMKS-ABE scheme. In our scheme, we combine the verifiable of the correctness of outsourced private key with multi-keyword search based on attribute encryption. In the general group model, the security of keyword index is proved. Under the random oracle model, the cipher text is proved to be selectively secure. In this article we proposed VMKS-ABE scheme. In our scheme, we combine the verifiable of the correctness of outsourced private key with multi-keyword search based on attribute encryption. In the general group model, the security Since the security in the general group model is much weak than in the standard model, it is worth constructing verifiable and multi-keyword searchable scheme in the standard model.

8. FUTURE ENHANCEMENTS

The verifiable of the correctness of outsourced private key with multi-keyword search based on attribute encryption. In the general group model, the security of keyword index is proved. Under the random oracle model, the cipher text is proved to be selectively secure.

9.REFERENCES

[1] M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.

[2] E.Punarselvam,"Bio-Medical Analysis of lumbar spine image using Gobar filter and canny edge detection algorithm of MRI", International Journal of Research in computer applications and Robotics,Vol.1 Issue No.8 Nov 2013 PP(42-50) ISSN:2320-7345.

[3] C. Metz. (2009, Oct.).DDoS attack rains down on Amazon Cloud [Online]. Available: http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/S

[4] K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput.Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

[5] E.Punarselvam,"Comparative analysis of Bio-CAD Technique and Canny Edge detection Algorithm for Lumbar spine images using Finite Element Method", International Journal of Engineering Research and Management, Vol. 1 Issue No.8 November 2014 PP(165-168) ISSN:2349-2058..

[6] J. Li, Q.Wang,C.Wang,N. Cao,K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," *International Journal of Engineering Research and Applications,* vol. 4, no. 7, pp. 441-445, May 2014, doi: 10.1109/INFCOM.2010.5462196.

[7] W. Sun, S. Yu, W. Lou, Y. Hou, and H. Li, "Protecting Your Right: Verifiable Attribute-BasedKeywordSearchwith Fine-Grained Owner- Enforced Search Authorization in the Cloud," *IEEE INFOCOM*, vol. 27, no. 4, pp. 226-234, Jul. 2014, doi: 10.1109/INFOCOM.2014.6847943.

[8] Dr.E.Punarselvam,"Robust Data Collection with Multiple Sink Zone In 3-D Underwater Sensor Networks", in International Journal on Applications in Basic and Applied Sciences, vol. 5, Issue no. 1, December 2019,PP 8-14.ISSN 2455 – 1007

[9] Y. Ye, J. Han,W. Susilo, T. H. Yuen, and J. Li, "ABKS-CSC: attributebased keyword search with constant-size ciphertexts," *Security & Communication Networks,* vol. 9, no. 18, pp. 5003-5015, Oct. 2016, doi: org/10.1002/sec.1671.

[10] Dr.E.Punarselvam,"Effective and Efficient Traffic Scrutiny in Sweet Server with Data Privacy", International Journal on Applications in Information and Communication Engineering Volume 5 : Issue 2: November 2019, PP 1 – 5

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *In Advances in Cryptology – EUROCRYPT,* Cramer R. Eds. Berlin, Germany: Springer, 2005, pp. 457-473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute -based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun.Secur.(CCS),* New York, NY, USA: ACM, 2006, pp. 89-98.

[13] E.Punarselvam, "Privacy and Secured Multiparty Data Categorization using Cloud Resources", International Journal of Innovative Research in Science, Engineering and Technology, ISSN(Online) : 2319 – 8753,ISSN (Print) : 2347-6710 Vol. 4, Special Issue 6,May 2015,pp 336-343 [14] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," In Public Key Cryptography – PKC, D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi Eds. Berlin, Germany: Springer, 2011, pp. 53-70.

[15] Dr.E.Punarselvam,"Heart Attack Recognition and Heart Rate Monitoring System Using IOT",in International Journal on Applications in Engineering and Technology, Vol. 5, Issue no. 2, December 2019,PP.5-10.ISSN 2455 - 0523