International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure Keyword Search Mechanism for Data Sharing in Cloud Computing

[1]Fariya Tabassum, [2] Dr. V. Bapuji

[1] PG Scholor, Vaageswari College of Engineering, Karimnagar – 505 527, India

[2] Professor & HOD, Department of MCA, Vaageswari College of Engineering, Karimnagar – 505 527, India

A B S T R A C T

Hardware and software expenses in computer infrastructure have been greatly lowered because to the advent of cloud infrastructure. To ensure security, the data is normally encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is tough to search and share the data after encryption. Nevertheless, it is a key responsibility for the cloud service provider as the users expect the cloud to do a speedy search and return the result without sacrificing data confidentiality. To tackle these challenges, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The suggested system not only provides attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two aspects. Additionally, the keyword in our scheme can be modified throughout the sharing phase without interacting with the PKG. In this paper, we discuss the notion of CPAB-KSDS as well as its security model. As an added bonus, we provide a concrete strategy and show that it is secure in the random oracle model against both the chosen ciphertext attack and the chosen keyword assault. Finally, the comparison of performance and properties shows that the proposed structure is both practical and efficient.

KEYWOEDS: Cloud Computing , Ciphertext-Policy Attribute Based Mechanism with Keyword Search and Data Sharing (CPAB-KSDS), PKG, Encryption, Attribute Based Encryption.

1. INTRODUCTION

1.1. BACKGROUND WORK

As a term, "cloud computing" encompasses both the software and the underlying infrastructure of remote servers and networks that are used to provide on-demand access to shared resources over the internet. Historically, "Services" have been referred to as "Computer Code as a Service" (SaaS). The Cloud is the collective noun for the software and infrastructure of data centres. The term "Public Cloud" is used to describe a Cloud that is made available to the public on a pay-per-use basis. Utility Computing is the product being offered. Amazon Web Services, Google App Engine, and Microsoft Azure are all examples of utility computing that are available right now. When referring to internal datacenters of a company or other organisation, the term "private Cloud" is typically used. This means that Cloud Computing encompasses both SaaS and Utility Computing but typically excludes private Clouds. The word "cloud computing" is used interchangeably; it should be replaced only if necessary for clarification. Fig. The diagram in 1.1 illustrates how people participate in Cloud Computing as either consumers or providers.

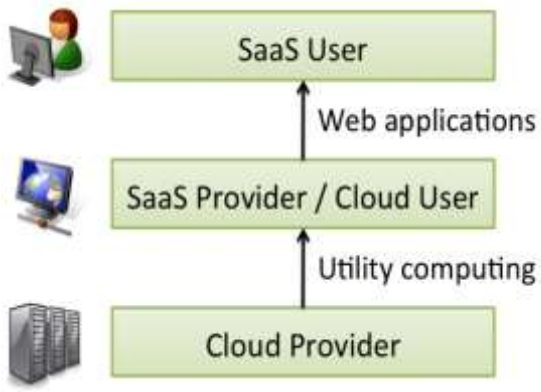

Fig: 1.1. User and Providers of Cloud Computing

To improve a networking infrastructure that incorporates all types of resources, usage areas, etc., falls under the purview of future Internet research and development. Cloud-based technology research is, thus, crucial to the long-term success of the Internet. Like the clever consequence of the re-marking explosion a few years ago, questions about the future of the Internet and the distributed computing that will power it sometimes arise from the vast range of traits assigned to "mists." Most cloud frameworks, therefore, centre on hosting applications and data on remote PCs, with the help of special replication procedures to ensure accessibility and ultimately achieving a heap-adjusting degree of adaptability. However, the practical model of clouds goes beyond such a fundamental technical approach, leading to difficulties analogous to those of the limitless Internet, albeit with slightly unusual focus due to the unique blend of ideas and goals inherent to cloud systems. Similar to an automatic yes vote based on a financial proposal, cloud frameworks would provide features that enable major components of the Internet to function without any restrictions.

Figure 1.2 illustrates the four distinct categories of cloud services available to businesses and organisations today. Some products offer Internet-based administrations including storage, middleware, coordinated effort, and database capacities targeted directly at customers.

Software as a service, sometimes known as SaaS, is a model for distributing programmes over the Internet. The user can choose how long they'd like to utilise the programme for and is charged appropriately.

PaaS services charge customers on a pay-per-use basis for access to their hosted platform. The user is at liberty to make as much or as little use of the Platform as they see fit.

Full IT support in the form of a service is provided by IaaS products, which the user can pay for on an as-needed basis..

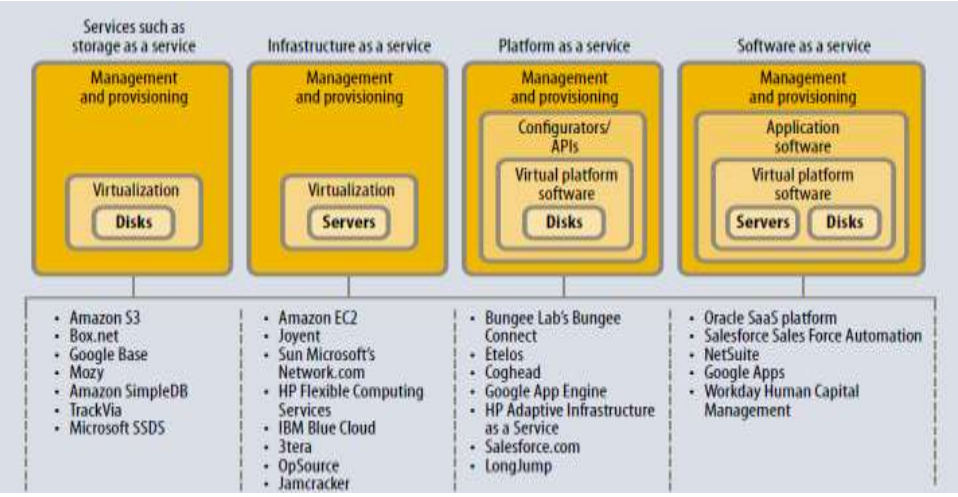

Fig: 1.2. Types of Cloud Service

2. OVERVIEW OF CLOUD COMPUTING

Distributed computing is a casual expression used to depict an assortment of various figuring ideas that include countless that are associated through a constant correspondence network(typically the Internet). Distributed computing is a language term without a generally acknowledged non-equivocal logical or specialized definition. In science, distributed computing is an equivalent word for circulated processing over a system and means the capacity to run a program on numerous associated PCs in the meantime. The notoriety of the term can be ascribed to its utilization in advertising to offer facilitated benefits in the feeling of use administration provisioning that run customer server programming on a remote area.

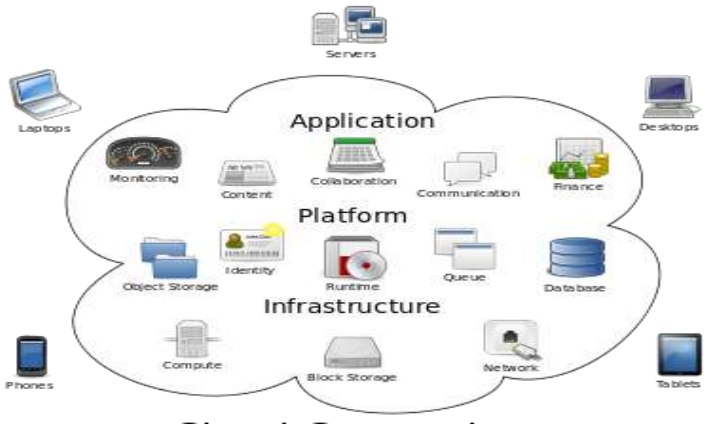

Fig: 2. 1. Cloud Computing

Some Traffic Redundancy Elimination are ushering in the era of distributed computing, which is the expansion and application of computer technology via the Internet. With the advent of Software as a Service (SaaS) registration technology and increasingly affordable and powerful processors, server farms are being transformed into massive data centres with the ability to manage large amounts of data computationally. With ever-faster data transmission rates and more stable but malleable network connections, it is now feasible for customers to subscribe to premium services that rely only on data and applications housed in off-site data centres.

3. PROPOSED WORK

Initially a ciphertext-policy attribute-based approach is applied for encrypted cloud data that includes a keyword search and shared facts. In the ciphertext-policy configuration, both the looking-out and sharing performances are enabled. Additionally, our method aids in keeping the keyword current all through the distribution stage. After detailing how our technique is constructed, we demonstrate that it is secure against CCA and CKA in a random oracle setting. In terms of both overall performance and property comparison, the planned building has been found to be both realistic and environmentally benign.

4. PROPOSED ARCHITECTURE

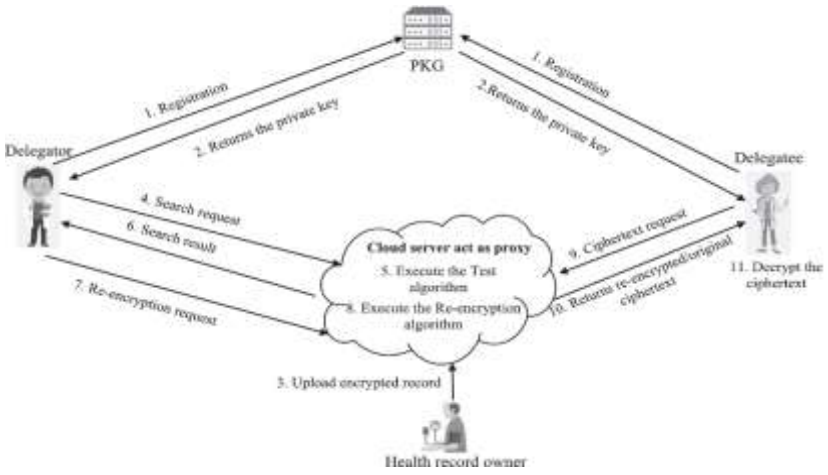

Fig: 4.1. System Model

5. ARCHITECHTURE/ IMPLIEMENTATION

In this architecture there are five modules

- Health Record owner
- Delegator
- Delegate
- Cloud Server
- PKG

PKG, cloud server (proxy), owner of fitness file, delegator (receiver of unique ciphertext), and delegatee are the five components that make up the CPAB-KSDS system (recipient of the re-encrypted ciphertext). This section details the device's operational procedure.

The PKG is responsible for the initialization of the system. PKG generates both the public parameters of the device, which are accessible to all members of the device, and the private parameters of the device, which are used to store the master secret key.

In the section devoted to registration, the PKG is used to complete the process. When a user submits an application for registration, the PKG creates a private key that corresponds to the user's attributes.

Ciphertext Upload: The owner of a private fitness report encrypts his file using the policy of the intended receiver and the keyword, and then uploads it to a cloud server.

In ciphertext search, the request for a search is composed of a search token generated by the recipient and sent to a cloud server. The recipient requests a search of the ciphertext, and the cloud server performs the search using the Test algorithm and sends back the results.

The delegator will then generate a new encryption key and send a request to the cloud server for re-encryption along with the new key. Using a different access policy, the cloud server re-encrypts the original document. Decryption occurs when the recipient (either the delegatee or the delegator) requests a

ciphertext from the cloud server, which is subsequently encrypted again using his private key. It is important to keep in mind that a delegatee might also serve as a delegator for other participants.

6. CONCLUSION

In this work, another thought of ciphertext-strategy property based instrument (CPAB-KSDS) is acquainted with help catchphrase looking and information sharing. A substantial CPAB-KSDS scheme has been built in this paper to demonstrate its CCA security in the arbitrary prophet model. The proposed plot is shown productive and useful in the exhibition and property examination. This paper gives a confirmed response to the open testing issue brought up in the earlier work [36], which is to plan a property based encryption with watchword looking and information sharing without the PKG during the sharing stage.

Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

REFERENCES

[1]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457–473, Springer, 2005.

[2]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, 986 pp. 89–98, Acm, 2006.

[3]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute988 based encryption," in Security and Privacy, 2007. SP'07. IEEE Sympo989 sium on, pp. 321–334, IEEE, 2007.

[4]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography, pp. 53–70, Springer, 2011.

[5]. H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," International Journal of Information Security, vol. 14, no. 6, pp. 487–497, 2015.

[6]. J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryp999 tion," Future Generation Computer Systems, vol. 52, pp. 67–76, 2015.

[7]. L. Fang, W. Susilo, C. Ge, and J. Wang, "Interactive conditional proxy re-encryption with fine grain policy," Journal of Systems and Software, 1002 vol. 84, no. 12, pp. 2293–2302, 2011.

[8]. M. Rajendra Prasad, V. Bapuji, and R. Lakshman Naik, "Cloud Computing: Research Issues and Implications," International Journal of Cloud Computing and Services Science(IJ-CLOSER), Vol. 2, Issues 2, Pages 133-139, ISSN: 2089-3337.