IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9679

Encrypted Data Storage vs Data Against Unauthorized Access

Nagesh R[1], Sowmya M S[2]

Student, Department of MCA, Bangalore Institute of Technology, Bangalore, India[1]

Asst.Proffessor, Department of MCA, Bangalore Institute of Technology, Bangalore, India[2]

Abstract: In the past, cloud computing offered a wide range of services and various advantages. The term "the cloud" refers to a method of storing large amounts of data online. There are also concerns about privacy and security when it comes to cloud computing. When providing critical information to third parties, the best way to minimise the effect of these concerns is to do so in an encrypted manner. Encrypted storage protects data from unauthorised access, but also complicates routine procedures that are nevertheless critical to carry out in order to keep the data safe from unauthorised access. When conducting online research, keywords are an essential part of the process. Based on how many keywords you require, you can put anywhere from two to five.

Keywords: Cloud, Security, Encryption, Privacy, Keywords.

I. INTRODUCTION

Using a wide-area network, users may connect to various computer resources via a cloud platform that is made available as a service (WAN). Schematic diagrams are commonly used to depict a system's design, and cloud-shaped symbols are a common addition. In cloud computing, the user's data, apps, and processing are all handled by third-party services that are located in other countries. Software and hardware that are hosted and provided over an Internet connection are known to as "cloud computing" in this technical environment. The vast majority of these businesses offer cutting-edge hardware and software to their clients. Here, consumers may submit files that meet specific requirements and choose an auditor to verify the correctness of content that has been hired. We are attempting to solve an issue with cloud - based data morality by suggesting attributes.

In this paper "Encrypted-Based Data Storage" is a technique that allows us to store encrypted data in a cloud storage. We've developed a new secure search protocol to keep cloud servers from deducing the true meaning of keywords or trapdoors in search results. For this reason, the encryption keys for each file and keyword are unique, allowing for the search of encrypted files with multiple keywords.

II. RELATED WORKS:

Jaydip Sens et al [1] they explored cloud computing's legislative, security, and privacy difficulties. Some solutions are proposed along with a brief presentation on potential cloud computing implementation patterns [1]. Cryptography secures information and contact with outside parties. A plan is offered to prevent attackers from reading, deleting, or manipulating users' cloud-stored data by encrypting it [2]. Cloud providers must protect customer data from unauthorized access and disclosure. Encrypting data on the client side before saving it in cloud storage is one way, but it's too burdensome. Since administrators can use both services for maintenance, the cloud storage provider's security service may be compromised [2, 3]. Vijay Varadarajan et al[4] proposed that they offer a secure RBE-based hybrid cloud storage architecture that allows an organisation to store data securely in a public cloud and sensitive information in a private cloud. Access control policies and techniques are needed to let users control their cloud-stored data [4]. For security, important information should be encrypted. A Cloud Secure Storage Mechanism combines information scattering and encoding to store cloud information and keys in pieced figure texts[5]. On this premise, client secret key and mystery sharing protect keys. Umarani Chellapandy et al [7] tested CSSM-supported OpenStack Swift. It has basic features like information search. Cloud Computing must secure, protect, and process user data. Data and transmission must be encrypted [6]. If you need to share sensitive or secret information between a browser and a web server, Encryption is an apparent method to protect communication. Venkata Sravan Kumar Maddineni et al [6] addressed that as more firms employ Cloud resources. Regenerative coding recovers ruined cloud data. Distributed storage is a secure, flexible, and efficient way to share information across group members [8]. Unreliable cloud services occur from software or hardware failure, unlawful access, and deliberate data loss or corruption. We present a new remote data

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9679

ownership verification strategy to audit encrypted shared data in each group. This system minimises encryption complexity and processing time [9]. Unauthorized users can unfairly access Data Warehouse data [10]. Cloud data confidentiality is very crucial, hence we present an Data security and integrity in cloud storage operations. Existing systems encrypt all data using the same key size, which increases cost and processing time. This paper discusses mobile security and storage [11].

III. METHODOLOGY

Because of our authentication approach, attackers cannot spy on the secret key and pretend to be unauthorized owners doing searches, but they are also authenticated and cancelled. [1]. In addition, the cloud server may do secure keyword searches without knowing the real data of keywords and trapdoors. In addition, the owner can secure terms using keys that they choose themselves, and users can do searches without knowledge of these keys.. [2]. AOPPF allows data owners to pick from a variety of functionalities while still enabling the server to arrange data in an appropriate manner. Reliability ratings may now be kept private thanks to this new feature. [3]. In order to establish how well our tactics work, we use real-world datasets to evaluate them. [4].

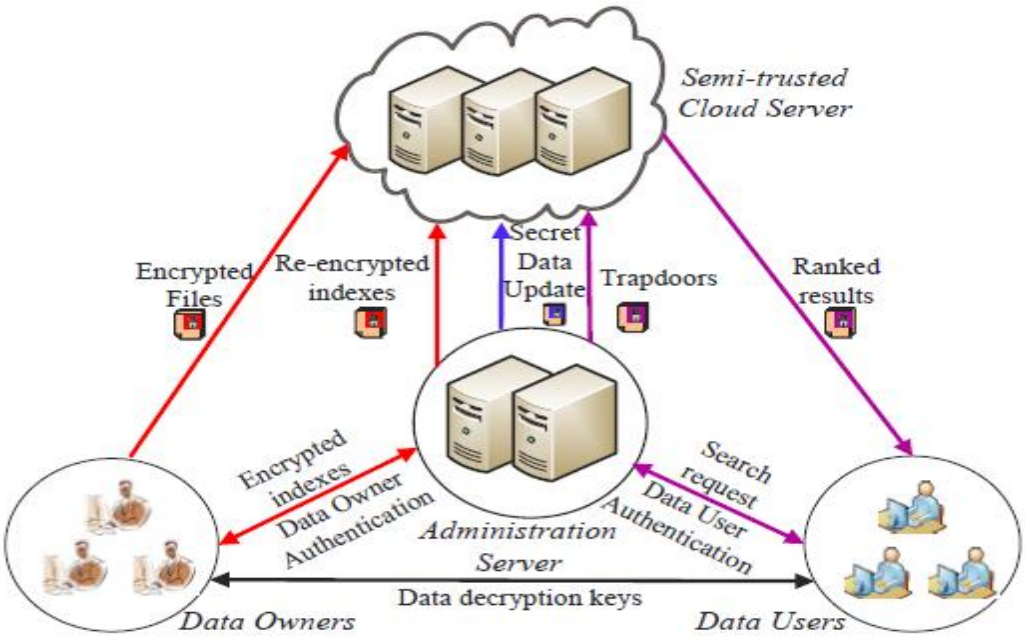

Fig. 1.Model of the System [1]

IV. FUTURE SCOPE

The cloud server will have the ability to select just the common attributes to be exposed as a component of the Section 4 design while it is carrying out the procedures for auditing protocols. They are going to investigate a method of auditing that guarantees there will be no knowledge gained at any point throughout the auditing process. In the next stage of research, the primary focus will be on developing a physical framework that is not only do able but also very efficient.

V. RESULTS

A comparison of the suggested capabilities to other relevant protocols is shown below. Front-end JavaScript, back-end SQL Statements are used to build the app. Both are essential to the project's advancement. NetBeans 8.2 and MySQL 5 are being used to develop the project. The performance graph of a system that were loaded from Google was presented using bar charts. When new packages are added to the system, this graph shows how rapidly the entire system functions. The more characteristics an identity has, the longer it will take to extract the user's secret key since the user's secret key is calculated for every attribute in the attribute set of the user. We measured the amount of time it takes to generate a ciphertext for a file. A collection of 10 attributes may be used to establish an unique user's attributes, and a file size of 1MB [1] is permitted. The speed at which a file is uploaded to the cloud relies on the current internet upload speed on the machine.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9679

CONCLUSION

This paper analyses strategies for cloud services multi-keyword search security. Our solution enables authorized data consumers to execute secure, simple, and successful searches across numerous data owners. We need a new dynamic secret key generation and an authentication system to authorise users and detect attackers who have hijacked the secret key and are undertaking unlawful searches. A new safe search protocol will let cloud servers search encrypted data using separate secret keys. Order and private information functions can sort search results by protecting keyword or file relevance scores. Our method works well with massive datasets and keyword sets. Future priorities include a multi-owner paradigm safe fuzzy search words challenge. Our solution will use commercial cloud services.

REFERENCES

[1]Jaydip Sens, ”Security and Privacy Issues in Cloud Computing”

[2] Madhumala RB, Sujan Chettri, Akshatha KC, ”Secure File Storage and Storing on Cloud using Cryptography”, International Journal for Computer Science and Mobile Computing,Volume 10,Issue 5,May 2021,ISSN:2320-088X.

[3] Rahul K, ”Data Storage Security in Cloud Computing Using Third Party Auditor(TPA) “, International Journal for Engineering Sciences and Research Technology,
ISSN:2277-9655.

[4]Vijay Varadarajan,”Achieving Secure Role-Based Access control on Encrypted Data in Cloud Storage”,Researchgate.net,No:260299380.

[5]Chiranjeevi P, ”Securing Privacy for Remote Data in a Cloud Storage”, International Journal of Advanced Research in Computer and Communication Engineering, Volume 10,Issue 7,ISSN:2278-1021.

[6]Venkata Sravan Kumar Maddineni, ”Security Techniques for Protecting Data in Cloud Computing”, School of Computing, November 2011.

[7]Umarani Chellampanndy, ”A cloud secure storage Mechanism based on Encryption and Dispersion”, International Research Journal of Modernization in Engineering Technology and Sciences ,Volume 4,
Issue 3 ,ISSN:2582-5208.

[8]Muthi Reddy P,”A Secure Data Sharing in Cloud Computing”, International Journal of Computer,ISSN:2307-4523.

[9]Chunxia Han,”Public Integrity Auditing of Shared Encrypted Data within Cloud Storage Group”,ID:1493768.

[10]Gaurav Kumar, ”Data Prevention from Unauthorized Access by Unclassified Attack in DataWarehouse”,ID:262494525.

[11]Lo ai Tawalbeh,”A Secure Cloud Computing Model based on Data Classification”, Procedia Computer Science,1153-1158.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License