e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707175 |

Two-Step Authentication Mechanisms for Cloud Content Delivery and Storage

Mrs. Barnali Chakraborty, Sudeep S A

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: A revolutionary advancement in distributed computing is currently tackling the worldwide issue of information storage. Distributed computing emerges as a rapid and effective solution for managing data storage and retrieval. Security remains a top priority in distributed computing, driving this investigation into a new method for access control. This approach introduces a secure access control system specifically designed for distributed computing environments. It leverages a clock and evolutionary framework to enhance precision in managing access. This innovative method facilitates seamless operations like uploading, downloading, and deleting files to and from the cloud. Essential concepts integral to this research encompass Cloud Computing, Cloud Privacy, and Access Control.

KEYWORDS: RAM, cloud computing

I. INTRODUCTION

The field of distributed computing is one that is currently developing. It deals with a fundamental shift in viewpoint in the dissemination of frameworks [8]. According to the National Institute of Standards and Technology [3], "Distributed computing is a model for enabling pervasive, advantageous, onrequest network access to a common pool of configurable computing assets (e.g., networks, servers, capacity, applications, and administrations) that can be quickly provisioned and delivered with minimal administrative effort or specialised organisation connection." This In ubiquitous administrations, where anybody may use PC administrations through the internet, distributed computing offers several benefits. Distributed computing allows you to build a device with a tiny display, processor, and RAM. There is no requirement for special equipment, such additional memory. It will reduce the size of our new technological devices. It also reduces the price of our framework. Distributed computing is exemplified through virtualization, on-demand configuration, Internet administration distribution, and open source programming [1]. The figure below shows the distributed computing model.

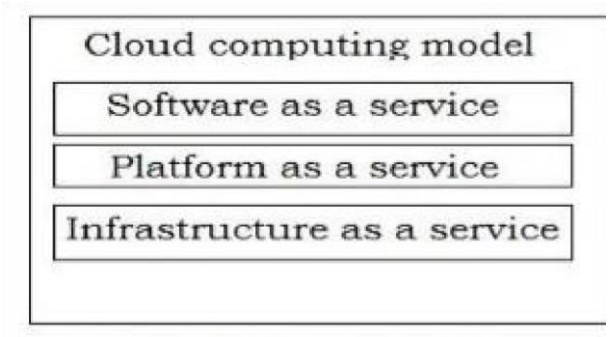

Fig 1: Cloud Computing Model

a) **SaaS-** to utilise the supplier's cloudbased applications, which may be used from a number of client devices via a straightforward client interface, like a Web application.
b) **PaaS-** Using the programming languages and tools supplied by the provider (java, python,.Net), uploading customer-made applications to the cloud
c) **IaaS**- establishing handling, capacity, organisations, and other fundamental figuring resources where the client may provide and execute ad hoc programming, such as functional frameworks and apps.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707175 |

Attacks against distributed computing have increased along with the emergence of cloud services. There are three primary attacks on cloud: [1], [2], and [3]. Attacks involving Denial of Service (DoS)
a) Attacks on side channels
b) Attacks on authentication
c)Man-in-the-Middle cryptographic attacks
d)Attacations at work
We urgently need a more sophisticated distributed computing security strategy as a result of these attacks. A technique or method for controlling access to a framework is known as access control [7]. Additionally, it could catch someone trying to get into an unauthorised system.

One programme can rely on another's identification thanks to access control [8].
Cloud-based systems are unable to implement the conventional access control approach known as application-driven access control [1], in which each programme oversees and controls its own set of clients. We'll need a lot of RAM to keep the client's specifics, including their username and secret phrase, because this technique requires a lot of memory. Because of this, a client-driven access control system is required for the cloud, in which each client request to any specialised organisation is loaded with the client's identity and permission information.

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control are the three basic types of access control models (RBAC)

We presently have a large number of access control processes in distributed computing. On the other hand, they cannot be acquired and are ineffective. We are aiming to provide a novel and improved access control method for distributed computing as a result of this issue.

II. RELATED WORK

In the next section, we look at the many access control methods that have already been put out by others. We will next go over our suggested approach for access control in distributed computing. Another important strategy for access control is FADE, which was presented by Y.Tang and associates [5]. The method in [5] enables fine-grained admission control and assured erasure for re-appropriated information on the cloud. This tactic isn't truly required, though. It is a good idea if the information owners and specialty cooperatives are nearby. Another access control scheme is HASBE [2] by Z.Wan, J.Liu, and R.H.Deng. The biggest drawback of [2] is that it is not customizable in compared to other systems. S.Yu and associates provide a distributed computing access control system. In this method, they employ PRE (Proxy Re-Encryption) and KPABE (Key Policy Attribute Based Encryption) [10]. Due to the growing complexity of encryption and decoding, this approach cannot be modified. A distributed computing technique for transient access is presented in [6 by Y.Zhu and coworkers. These methods are limited to frameworks in [6] where data owners and specialist coops are housed in the same enclosed location. M.Li and his team's contribution [4], which explains the other main storyline, is available online. However, the plan is pricey. In an IEEE TransCom-11 International Joint Conference, M.Zhou and his coworkers provide a method for privacy-preserving access control for distributed computing [9]. There are a few downsides to this method [9]. However, the lack of flexibility and adaptability in this approach makes it useless.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707175 |

III. PROPOSED SCHEME

A. The creation of our suggested model. Our suggested model has a progressive architecture, as seen in Figure 2.

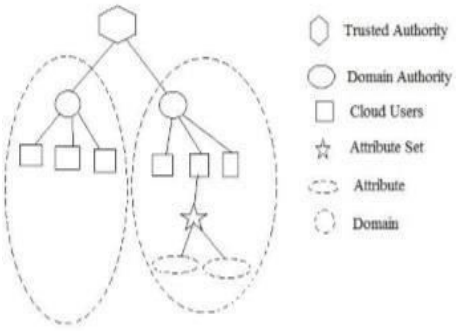

Fig 2: System Structure

This innovative structure's cornerstone of faith is the believed power, which approves eminent space experts. Furthermore, this high-level subject specialist approves the cloud clients. We take into account both the owners and the clients as a cloud client. For each cloud client, our system keeps a characteristic set that includes a number of attributes unique to that client. In accordance with the client, it could alter. A space consists of one area authority, several cloud customers, and many. Additionally, we time the key production process using a clock. **A. Framework Model.**

Our method's real-world model is shown in Figure 3. This model has a total of four pieces. Owner of the cloud, client of the cloud, the clock, and the unreliable cloud

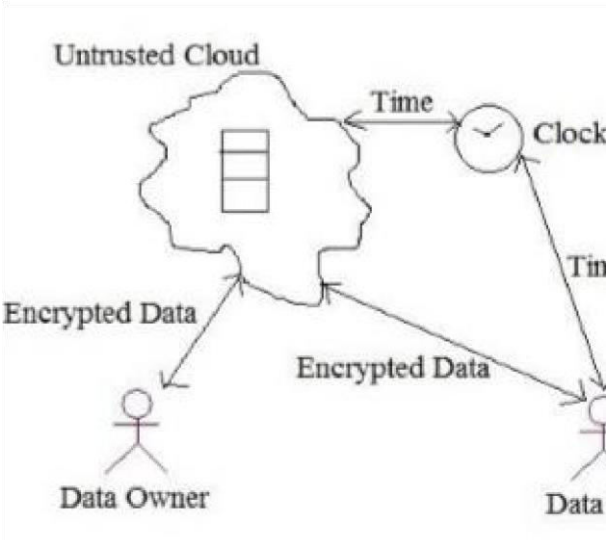

Fig 3: System Model

From here, the data's owner can upload it to the cloud. He will immediately scramble the document and move it to the unreliable cloud to make his record as unreliable as possible. The records can only be decrypted by the owner of the data. The transmitted data is therefore secure in the dubious cloud. An information client sends a request to the cloud whenever it needs to access a record stored there. The request will then be forwarded to the owner by the cloud. The proprietor will then examine the client's unique setup. The owner will send a key to the customer if they possess a lot of qualities. The timer will begin ticking once The owner mails a key to the customer. After a predetermined length of time, that key expires. As a result, the customer is required to finish the desired paper before the deadline.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707175 |

B. Fundamental tasks of the proposed model

1. Registration

To carry out any operation in the cloud, both the client and the owner must enrol. The customer and the owner will submit an enrollment request for enrolment to the comparable space authority. After then, the space authority certifies that the new component complies with the agreements. The area authority will send the request to the enclosed space if they are ready to abide by the conditions. Then, the thinking power will provide everyone of the owners and customers an extraordinarily durable ID. Once that is done, they will be able to make a private key for them.

2. Document Upload

The owner of the information must first encrypt a document with his private key before sending it to the following higher level. The jurisdictional authority is that. The local government will then check to see if the proprietor is registered. The space authority will deliver the encoded record to the trusted authority if he is a registered owner.

3. Document Download

The information client must first make a request to his designated space authority in order to retrieve any record from the cloud. The local authority will then inspect the customer. The request will be sent to the trusted in authority if the customer is genuine. The owner of the pertinent data will then get this request from the supposed power. The owner will then look through the client's trait profile. The owner will send a key to the customer if they possess a lot of qualities. When the owner provides a client a key, the clock will begin to run. After a predetermined length of time, that key expires. Therefore, the customer is required to finish the specified paper within the specified time frame.

4. Document Deletion

The only person who may remove data from the cloud is the owner of that data.

The believed power will assign an ID number to each information proprietor throughout the enrollment period. These identification numbers endure a very long time for them. In a similar vein, each of them possesses a short-lived secret key. The information owner must first submit a request to his relevant space authority in order to remove a document. This solicitation contains the proprietor id and document name. The local government will next ask the owner for their secret phrase. If the owner provides the right secret word, the local authority will forward the deletion request to the trusted authority. The document will then be removed from the cloud by the supposed power.

IV. CONCLUSION

This approach presents a highly effective method for access control in cloud computing. It utilizes a clock-based system to generate time-based decryption keys and incorporates a hierarchical framework to guarantee strong security and accurate access management within cloud environments. The core operations supported by this approach include uploading, downloading, and deleting files.

REFERENCES

1. Y.G.Min, Y.H.Bang, “Cloud Computing Security Issues and Access Control Solutions”, Journel of Security Engineering, vol.2, 2012.
2. Z.Wan, J.Liu, R.H.Deng, “HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing”, IEEE Transactions on Forensics and Security, vol 7, no 2, APR 2012.
3. P.Mell, “The NIST Definition of Cloud Computing.” U.S. Department of Commerce:Special Publication 800-145.
4. M.Li, S.Yu, Y.Zheng, K.Ren, W.Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” IEEE Transactions on Parallel and Distributed Systems, vol 24, no 1, JAN 2013.
5. Y.Tang, P.P.C.Lee, J.C.S.Lui, R.Perlman, “Secure Overlay Cloud Storage with Access Control and Assured Deletion,” IEEE Transactions on Dependable and Secure Computing, vol 9, no 6 NOV/DEC 2012.
6. Y.Zhu, Hu, D.Huang, S.Wang, “Towards Temporal Access Control in Cloud Computing,” Arizona State University, U.S.A.
7. A.R.Khan, “Access Control in Cloud Computing Environment,” ARPN Journal of Engineering and Applied Sciences, vol 7, no 5, MAY 2012.
8. B.Sosinsky, “Cloud Computing Bible,” , Ed. United States of America: Wiley, 2011.
9. M.Zhou, Y.Mu, W.Susilo, M.H.Au, “Privacy-Preserved Access Control for Cloud Computing,” IEEE International Joint Conference, 2011

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com