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

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

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: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207157 |

Divided Control Access is used in Cloud Computing

Kalyane Krashnakant Shivajirao[1], Prof. Seema Nagaraj[2]

P.G. Student, Department of Master of Computer Application, Bangalore Institute of Technology, Bengaluru, Karnataka, India

Assistant Professor, Department of Master of Computer Application, Bangalore Institute of Technology, Bengaluru, India

ABSTRACT: A key innovation is emerging with distributed computing. Everyone on the planet faces a serious problem with information storage. If you're seeking for the quickest and simplest method of storing and retrieving data, distributed computing is a fantastic solution. In distributed computing, security comes first. I wish to demonstrate a novel method for providing access control for distributed computing in this work. This design offers secured admission control for distributed computing. It uses a clock and a progressive design to enable more precise access control. Using this technique, we may transfer, download, and delete documents to and from the cloud with ease. Cloud Computing, Cloud Privacy, and Access Control are just a few of the terms in the collection.

I. INTRODUCTION

Computerized sharing is a field that is still in development. It talks about a major shift in perspective in the spread of frameworks [8]. Distributed A strategy for enabling is computing. widespread, advantageous, on-request access to a network via shared pool of computational options assets, such as networks, servers, capacity administrations, programs, and apps that quickly provisioned and delivered with little administrative effort or accordance to the affiliation with a specialized organization National Institute of Standards and Technology [3]. This The benefits of distributed computing are numerous. in ubiquitous administrations, where anyone can use PC administrations online. You can create a gadget with a tiny display, processor, and RAM thanks to distributed computing. No specialized hardware, such as increased memory, is required. It will become smaller. A diagram of the distributed computing model is shown below.

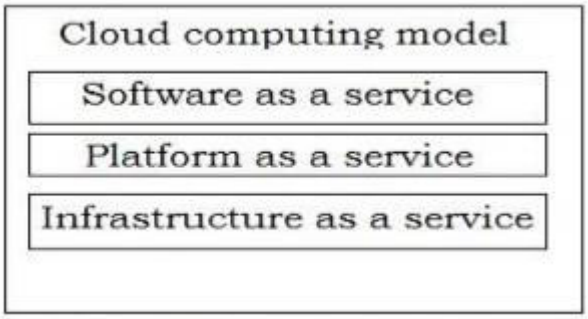

Fig 1: Cloud Computing Model

a) SaaS - using the vendor's cloud-based apps, which may from a variety of client devices via a simple client interface, similar to a Web application.
b) PaaS - Uploading user-created apps to the cloud using The vendor's programming languages and resources (java, Python, and.Net).
c) Infrastructure as a Service (IaaS) – supplying organizations, handling, capability, and other important resources where the client may give and execute ad hoc programming, such as programs and frameworks that are useful.
Attacks on distributed computing have grown as cloud services have become more prevalent. On cloud, there are primarily three attacks: [1], [2], and [3].

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207157 |

Denial of service (DoS) attacks
Attacks against side channels, authentication, and man-in-the-middle cryptographic attacks are only a few examples. d) Conflicts on work
We urgently need a more sophisticated distributed computing security approach as a result of these risks. Using access control, you can regulate who has access to what information. It has access to a framework [7]. Furthermore, it might catch someone attempting to access an unauthorised system.
Access control allows one programme to rely on another's identity [8]. The traditional approach Cloud-based systems cannot use the type of access control known as application-driven access control [1], in which each program supervises and manages its own set of clients. We'll require a lot of RAM to store the data because this method consumes a lot of memory. client's information, such as their username and secret phrase. Since each client request to any specialist organisation must be loaded with the client's identification and permission information, a client-driven access control system is necessary for the cloud.
There are two types of access control: mandatory and discretionary.
The three fundamental categories of access control models (RBAC) include:

II. RELATED WORK

The various access control techniques that have already released by others are examined in the next section. Next, we will discuss our recommended strategy for access control in distributed computing. FADE is another significant access control approach that was introduced by Y.Tang and colleagues [5]. For re-appropriated information in the cloud, the solution in [5] offers fine-grained admission control and ensured erasure. However, this strategy is not actually necessary. If the information owners and the speciality cooperatives are close together, that is an excellent concept. HASBE [2], a method for access control, was developed by Z.Wan, J.Liu, and R.H.Deng. The main flaw with [2] is that it is not Comparable to other systems, customisable. An access control system for distributed computing is offered by S. Yu and others. They use KPABE (Key Policy Attribute Based Encryption) and PRE (Proxy Re-Encryption) in this method [10]. This strategy cannot be changed due to the increased complexity of encryption and decoding. Y.Zhu and colleagues offer a distributed computing method for transitory access in [6. These techniques are only applicable in frameworks described in [6] in which data owners and expert co-ops are housed in the same enclosed space. Online resources include the contribution [4] by M.Li and his group, which discusses the other key plot line. But the plan is expensive. An approach for privacy-preserving access control for distributed computing is presented by M. Zhou and his colleagues in an IEEE TransCom-11 International Joint Conference [9].

III. PROPOSED SCHEME

A. the development of our recommended model. Figure illustrates the progressive design of our proposed approach.

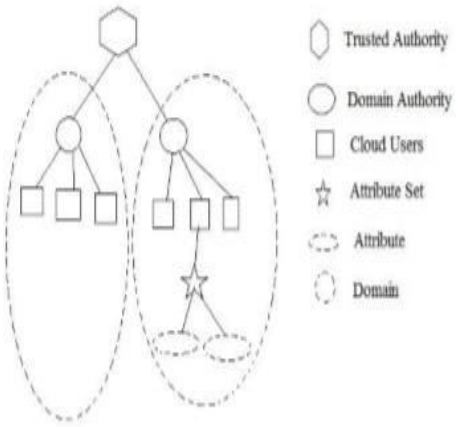

Fig 2: System Structure

The power that is thought to authorise prominent space experts is the foundation of faith for this creative construction. Furthermore, the cloud clients are approved by this high-level subject specialist. As a cloud client, we consider both the owners and the clients. Our system maintains a characteristic set for each cloud client that contains a number of specific

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207157 |

characteristics specific to that client. It could change depending on the client. One area authority, numerous cloud users, and many make up a space. We also use a clock to time the essential production process. 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.

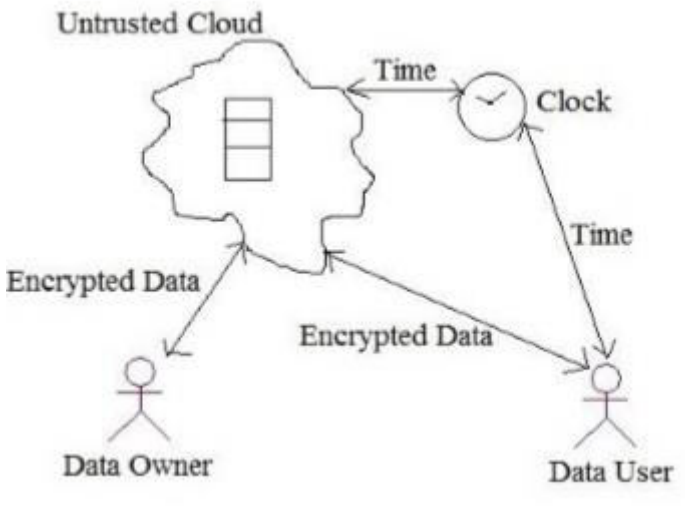

Fig 3: System Model

The owner of the data may upload it to the cloud from this point. To make his record as unreliable as possible, he will quickly scramble the document and transfer it to the unreliable cloud. Only the data owner is capable of decrypting the records. Therefore, the shady cloud is a secure place for the sent data. Anytime a client of information needs to access a record kept in the cloud, the client sends a request to the cloud. The cloud will then send the request on to the owner. The owner will then assess the client's particular configuration. If the client possesses a lot of traits, the owner will send them a key. Once the owner ships a key to the customer, the timer will start to run. Once a Fundamental tasks of the proposed model

1. Registration
2. Document Upload
Both the client and the owner must enrol in order to do any operation in the cloud. The client and the owner will send the equivalent space authority an enrollment request for enrollment. The space authority then confirms that the new component complies with the contracts. If the enclosed space is willing to comply with the requirements, the area authority will send the request to them. Then, the creative capacity will give each owner and consumer a really robust ID. They will be able to create a private key for them after that is finished.
3. Document Download
To obtain any record from the cloud, the information client must submit a request to his designated space authority first. The consumer will then be inspected by the local authority. If the customer is sincere, the request will be conveyed to the respected authority. The alleged power will then make this request to the owner of the relevant data. After that, the owner will review the client's trait profile. If the client possesses a lot of traits, the owner will send them a key. The clock will start when the owner hands a client a key. That key expires after a predetermined period of time. As a result, the buyer must complete the requested paper within the allotted time.4. Document
4. Deletion
The owner of the data is the only one who has the authority to remove it from the cloud. Each information owner will receive an ID number from the believed power throughout the enrolment period. They can use these identification numbers for a very long period. Similar to that, each of them has a temporary secret key. To remove a document, the information owner must first make a request to his designated space authority. The document name and proprietor id are included in this solicitation. The owner will then be questioned by the local authority regarding their code word. The local authority will send the deletion request to the trusted authority if the owner supplies the correct secret word. Following that, the document will be deleted from the cloud.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207157 |

IV. FUTURE ENHANCEMENTS

Fine-Grained Access Control: Explore advancements in access control models to provide even more fine-grained control over data access. Implement attribute-based access control (ABAC) or policy-based access control to allow for dynamic and context-aware authorization decisions based on user attributes and environmental conditions.
Multi-Cloud Support: Investigate the feasibility of extending the access control mechanisms to support multi-cloud environments. Develop solutions that enable seamless data sharing and access control across multiple cloud providers, allowing users to leverage resources from different clouds while maintaining consistent security measures.
Blockchain Integration: Consider integrating blockchain technology into the access control framework to enhance data integrity and transparency. Blockchain can provide an immutable record of access control decisions and enable decentralized control over data access, reducing the reliance on central authorities.
Privacy-Preserving Techniques: Explore privacy-preserving techniques, such as homomorphic encryption and differential privacy, to protect sensitive data while allowing for meaningful computations on encrypted data. These techniques can strengthen data privacy and security in cloud-based data storage and sharing scenarios.
User Behavior Analysis: Incorporate user behavior analysis and anomaly detection to enhance access control decision-making. By continuously monitoring user actions and behavior patterns, the system can detect suspicious activities and dynamically adjust access privileges accordingly.
Multi-Factor Authentication (MFA): Integrate multi-factor authentication methods, such as biometrics or hardware tokens, to bolster the authentication process and add an extra layer of security. MFA can reduce the risk of unauthorized access even in case of compromised credentials.
Secure Data Deletion: Implement secure data deletion mechanisms to ensure that data is thoroughly and irreversibly removed from the cloud storage when it is no longer needed. This is especially important to comply with data protection regulations and avoid potential data breaches.
Real-Time Auditing and Monitoring: Develop real-time auditing and monitoring capabilities to track and analyze access control events. Auditing logs can help identify potential security incidents, support forensic analysis, and assist in compliance auditing.
Federated Identity Management: Investigate the feasibility of federated identity management solutions to enable seamless authentication across multiple cloud-based services. This would simplify the user experience and reduce the need for redundant user account creations.
Continuous Security Assessments: Implement continuous security assessments to proactively identify vulnerabilities and potential security risks. Regular security assessments can help maintain the robustness of the access control system over time.
By exploring these future enhancements, the field of Dual Access Control for Cloud-Based Data Storage and Sharing can evolve to address emerging challenges and maintain a strong focus on data security, privacy, and efficient data sharing in cloud environments

V. CONCLUSION

This way of implementing access control for cloud computing is quite efficient. It has a hierarchical structure and makes use of a clock to generate a time-based decryption key. This paradigm ensures cloud computing security and access management. These three procedures—uploading, downloading, and deleting files—are the primary steps in this method.

REFERENCES

[1] Y.G. Min and Y.H. Bang, "Cloud Computing Security Issues and Access Control Solutions", Journal of Security Engineering, vol. 2, 2012.
[2] Z.Wan, J.Liu, and 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] Peter Mell, "The NIST Definition of Cloud Computing." Special Publication 800-145 from the U.S. Department of Commerce.
[4] "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] "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6 NOV/DEC 2012. Y. Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman.
[6] "Towards Temporal Access Control in Cloud Computing," Arizona State University, USA, by Y. Zhu, Hu, D. Huang, and S. Wang.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207157 |

[7] A.R. Khan, "Access Control in Cloud Computing Environment," ARPN Journal of Engineering and Applied Sciences, volume 7, issue 5, MAY 2012.
[8] B. Sosinsky, "Cloud Computing Bible," Wiley, 2011 (United States).
[9] "Privacy-Preserved Access Control for Cloud Computing," M. Zhou, Y. Mu, W. Susilo, and M. H. Au. International Joint Conference of the IEEE, 2011
[10] "Achieving Secure, Scalable, and Finegrained Data Access Control in Cloud Computing," by S. Yu, C. Wang, K. Ren

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

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