INTI JOURNAL | Vol.2024:21
eISSN:2600-7320

Dual Access Control for Cloud Storage and Sharing

Sandeep T.S.[1,*], Shreedhara N. Hegde [1], C. Pui Lin[2]

[1]DSATM Kanakapura Road, Udayapura, Bangalore Karnataka 560082,
[2]Faculty of Data Science & IT, INTI International University, 71800 Nilai, Malaysia

***Email:** sandeepshanth611@gmail.com

Abstract

In the field of distributed computing, a significant innovation is now being developed. The process of storing information is extremely difficult for every single person on the planet. Data storage and retrieval can be accomplished in the most straightforward and expedient manner possible through the utilisation of distributed computing. When it comes to distributed computing, security is the most important consideration. An alternative approach to provide access control for distributed computing is what this research work intend to illustrate. Distributed computing can benefit from this design's protective admission control. Additionally, it makes use of a watch and a progressive design in order to facilitate access control, that is more exact. It is possible for us to send, download, and erase papers to and from the fog with ease using this method.

Keywords

Cloud Computing, Cloud Privacy, and Access Control

Introduction

The domain of distributed processing is presently undergoing development. The paper discusses a significant change in perspective regarding the distribution of frameworks (Papoutsi, C., et al, 2024). The American National Standardization Institution (Zhang, Y., et al, 2021) defines distributed computing as a model that allows widespread and beneficial access to a shared pool of configurable computing resources (such as networks, servers, capacity, applications, and services) on-demand. These resources can be rapidly provisioned and delivered with minimal administrative effort or specialized organizational involvement. In the realm of widespread computer usage, where anybody can access computer services over the internet, cloud computing has numerous advantages. Distributed computing enables the construction of a device equipped with a compact display, processor, and RAM. There is currently no need for any specific equipment, such as new memorials. It will reduce the size of our innovative technological devices. Additionally, it reduces the cost of our framework. Distributed computing is demonstrated using virtualization, the ability to configure systems on-demand, the distribution of administrative tasks across the Internet, and the use of open-source programming (Li, J., et al, 2019). Below is Figure 1, which illustrates the distributed computing model.

Submission: 4 May 2024; **Acceptance:** 2 August 2024

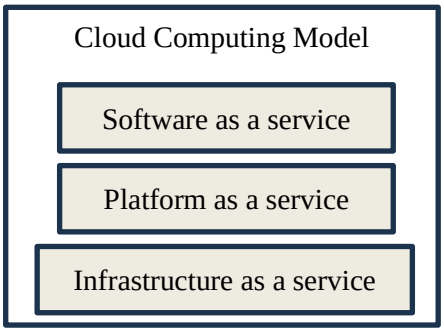

Figure 1. Cloud Computing Model

The depicted diagram comprises Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS enables the use of cloud-based applications provided by a supplier. These programs can be accessed from various client devices using a user-friendly client interface, such as a Web application. PaaS is a cloud computing service that allows users to utilize programming languages and tools provided by the service provider, such as Java, Python, and .Net. It enables users to upload their own apps to the cloud. Infrastructure as a Service (IaaS) is crucial for developing and managing essential computing resources, including handling, capacity, and organizations. It allows the client to provide and execute ad hoc programming, such as functional frameworks and apps.

The frequency of distributed computing attacks has risen in tandem with the growth of cloud services. Three main assaults on cloud infrastructure have been identified by Li et al. (2019), Wang et al. (2020), and Zhang et al. (2021). Denial of Service (DoS) assaults encompass side channel attacks, authentication attacks, man-in-the-middle cryptography attacks, and workplace attacks. The research requires an immediate implementation of a more advanced distributed computing security strategy in response to these assaults. The act of regulating access to a system is referred to as access control (Deng, R. et al., 2023). Moreover, it has the capability to detect anybody attempting to get access to an unauthorized system.

Access control allows one program to depend on the identification of another program (Papoutsi, C., et al., 2023). Cloud-based systems cannot utilize the traditional access control method called application-driven admittance controller (Li, J., et al, 2019), where each program manages and regulates its own group of customers. To save the client's specific information, such as their username and secret phrase, a considerable amount of RAM is necessary, as this strategy relies on a portion of memory. Therefore, a client-driven access control system is necessary for the cloud, wherein each client requests access to a certain organization by providing their identification and permission information. The access includes obligatory gate control (MAC), optional access control (DAC) and role-based access control are the three elementary kinds of approach manage forms (RBAC).

In the field of distributed computing, we are currently dealing with a significant number of access controller processes. On the other side, they are not able to be obtained and also do not offer any benefits. As a response to this problem, the team intended to develop a novel and improved access operate logic for distributed computing which will be a signature achievement.

Researchers have investigated dual access control as a layered security technique in cloud systems. Li et al. introduced a technique that merges attribute-based encryption (ABE) and proxy re-encryption (PRE) to achieve precise access control and secure delegation of decryption rights

in cloud storage (Li, J., et al, 2019). In another study, Wang proposed a system that utilises blockchain technology to improve the security and reliability of access control policies and user actions in cloud-based data sharing (Wang et al.,2020).

In another study, Zhang examined the implementation of hierarchical dual access control in cloud storage systems on a wide scale (Zhang et al., 2021). This approach involves granting varying levels of privileges to users based on their roles and responsibilities. Research on security risks related to cloud storage and sharing has significantly increased. Chen reported to utilised homomorphic encryption to facilitate secure sharing and collaboration of data while maintaining anonymity (Chen et al., 2017).

In addition to that, Liu examined the concept of privacy-preserving data sharing using searchable encryption, which enables keyword searches without disclosing the original text Liu et al., 2018) and Zhao concentrated on improving the efficiency of data retrieval by implementing a multi-keyword ranked search system (Zhao et al., 2022).

Researchers have investigated the incorporation of fog computing with cloud storage and sharing to improve security and performance. In their study, Deng introduced a fog-assisted approach to transfer computationally demanding activities from the cloud, thereby enhancing the efficiency and scalability of data sharing (Deng, R. H., et al, 2023).

Proposed Scheme

The process of developing our proposed model is depicted in Figure 2. As seen in Figure 2, the model that we have proposed takes a progressive approach to its architecture.

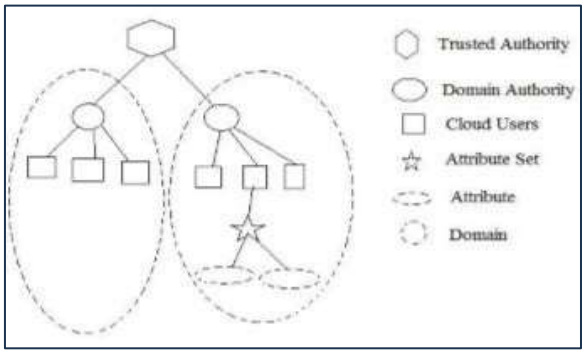

Figure 2. System Structure

It is the supposed power that gives approval to prominent space professionals, and it is the cornerstone of faith that this creative building is built upon. In addition, this high-level subject matter expert is responsible for regulating the cloud customers. When it comes to cloud clients, both the vendors and the customers are equally measured. This technique considers a characteristic set for each raincloud client. This set is comprised of several characteristics that are exclusive to that client. Depending on the requirements of the customer, it could change. The components that make up a space include a single area authority, multiple cloud clients, and many. In addition, we use a clock to keep track of the time during the critical production process.

A. Framework Model.

Figure 3 is a demonstration of the real-world model provided by our method. The structure is comprised of a total of four parts. The owner of the cloud, the cloud's client, the clock, and the cloud that is reliable are all included.

.

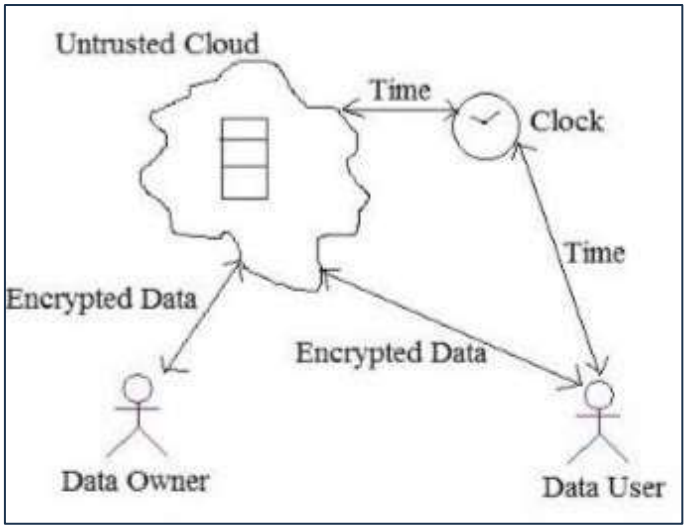

Figure 3. System Model

From this point, the individual who possesses the data can transfer it to the cloud. He will promptly encrypt the manuscript and transfer it to the untrustworthy cloud to maximize its unreliability. The records can only be deciphered by the data owner. The data that is sent is thus protected in the questionable cloud. A client sends an application to the raincloud anytime it requires retrieving a stored record. Subsequently, the rain cloud will transmit the request to the proprietor. The proprietor will thereafter evaluate the client's distinctive configuration. If the buyer possesses a multitude of traits, the proprietor will dispatch a key to them. The timer will commence counting down once the proprietor dispatches a crucial message to the client. Once a specific duration has passed, the key becomes invalid. Consequently, the customer must complete the needed paper prior to the deadline.

B. Fundamental tasks of the proposed model

(i) Registration

To do any form of control in the cloud, both the client and the landlord must register. The customer and the landlord have chosen to submit an enrolment request to the relevant space authority. Subsequently, the space authority verifies that the new component adheres to the agreements. If the area agency promptly complies with the conditions, they will transmit the application to the confined area. Subsequently, the cognitive ability will furnish each vendor and buyer with an exceptionally resilient identification. Once that task is completed, they will have the capability to generate a private key for themselves.

(ii) Document Upload

Prior to transmitting the document to the subsequent higher level, the information owner must encrypt it using their private key. The jurisdictional authority refers to the legal power or control that a particular entity or organization possesses. The local authorities will thereafter verify the proprietor's registration status. The space authorities will transmit the encoded record. If the individual is a person who has been officially acknowledged by a reliable owner of an organization.

(iii) Document Download

To access any records from the rain cloud, the customer must first submit a wish to their designated space authority. The local government will thereafter conduct an inspection of the consumer. If the client is authentic, the request will be forwarded to the anticipated person in a position of authority. The individual in possession of the relevant data will then get this application from the presumed authority. The vendor instructions involve examining the client's trait profile. If the customer possesses a multitude of attributes, the landlord will provide them with a keyboard. Once the holder gives a key to a client, the timer will start running. Once a specific duration has passed, the key becomes invalid. Hence, it is imperative for the consumer to complete the designated document within the stipulated timeframe.

(iv) Document Deletion

The owner of the data is the only one who can remove it from the fog. During the enrolment phase, each information proprietor will be assigned an ID integer by the believed power. For them, these identification numbers are quite durable. Likewise, every one of them has a transient secret key. To have a document removed, the information owner must first file a request to the appropriate space authority. The document name and proprietor ID are contained in this solicitation. Next, the owner will be asked for their secret word by the local government. If the owner provides the correct private phrase, the regional government will forward the removal order to the appropriate authorities. Following that, the purported power will erase the paperwork from the server.

Conclusion

The provision of a log-on mechanism for cloud computing is made possible through the utilization of this excellent technology. Along with having a hierarchical structure, it makes use of time to generate a time-based decryption key. This paradigm ensures that protection and approach control are maintained throughout the fog processing process. The primary procedures involved in this method are the uploading of files, the downloading of files, and the erasure of sleeves.

Acknowledgement

The researcher did not receive any funding for this study, and the results have not been published in any other sources.

References

Altaf, A., Iqbal, F., Latif, R., Yakubu, B. M., Latif, S., & Samiullah, H. (2022, July). A survey of blockchain technology: Architecture, applied domains, platforms, and security threats. *Social Science Computer Review*, *41*(5), 1172–1193. https://doi.org/10.1177/08944393221110148

Bharathi Murthy, C. V. N. U., Lawanya Shri, M., Kadry, S., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. *IEEE Access*, *8*, 1–1. https://doi.org/10.1109/ACCESS.2020.3036812

Chen, X., Li, J., Ma, J., & Lou, W. (2017). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Parallel and Distributed Systems*, *28*(6), 1702–1716. https://doi.org/10.1109/TC.2011.245

Deng, R. H., Lu, R., Lai, C. F., Zhou, T. H., & Lin, H. Y. (2023). Blockchain-based cloud storage: Architecture, challenges and opportunities. *Journal of Network and Computer Applications*, *209*, 103708. https://doi.org/10.1016/j.jnca.2022.103708

Li, J., Chen, X., Li, M., Li, J., Lee, P. P., & Lou, W. (2019). Enabling efficient multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems*, *30*(12), 2748–2762. https://doi.org/10.1109/TETC.2014.2371239

Liu, C., Chen, L., Chen, C., Wang, Y., & Yuan, J. (2018). Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates. *IEEE Transactions on Parallel and Distributed Systems*, *29*(9), 1906–1920. https://doi.org/10.1109/TPDS.2013.191

Renee, G., Kelani, Z., & Sean, D. Y. (2023, February). A novel application of blockchain technology and its features in an effort to increase uptake of medications for opioid use disorder. *Artificial Intelligence Advances*, *4*(2). https://doi.org/10.30564/aia.v4i2.5398

Wang, C., Ren, K., Lou, W., & Li, J. (2020). Toward publicly auditable secure cloud data storage services with efficient user revocation. *IEEE Transactions on Information Forensics and Security*, *15*, 1662–1675. https://doi.org/10.1109/MNET.2010.5510914

Zhang, Y., Deng, R. H., Choo, K. K. R., & Vasilakos, A. V. (2021). A survey on security and privacy issues of blockchain-based cloud storage. *Future Generation Computer Systems*, *115*, 129–148. https://doi.org/10.3934/mfc.2018007

Zhao, Y., Deng, R. H., Wang, X., & Choo, K. K. R. (2022). Blockchain-based public verification for cloud storage against procrastinating auditors. *IEEE Transactions on Cloud Computing*. https://doi.org/10.1109/TCC.2019.2908400