IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, November 2024

# SecureCloud: A Shield Against Virtual Threats

**Rakshitha M V[1] and Dr. Chitra K[2]**
Student MCA, IVth Semester[1]
Associate Professor, Department of MCA[2]
Dayananda Sagar Academy of Technology and Management, Udaypura, Bangalore, Karnataka, India
rakshithamv2001@gmail.com

**Abstract:** *Cloud computing is a constituent of today and tomorrow innovative information and computing technologies which provides useful and convenient services like storage and access etc. But it has important problems which aggravate with security aspects of a system with regards to the data confidentiality and integrity. These challenges are met in this paper by conducting a detailed theoretical study of literature on data security risks in single and multi-cloud models. Some of the threats include; break-ins, theft of information and loss of information. A comparison of extant literature on security measures like encryption and access control in the cloud based systems is done. It is shown that the solutions available currently have certain deficits, which contribute to the necessity of enhancing safety features. Thus, to fill these gaps, it is suggested to have one layer of protection against data access and another one in relation to data downloads. That way it is protective of the data, useful and clients' information privacy will be well protected. Thus, the results of the study can be valuable for researchers and cloud service providers who are working on the improvement of the information security in cloud environments.*

**Keywords:** Cloud computing, Cloud service provider, data security, Encryption

## I. INTRODUCTION

The flexibility and ability to save money in addition to a more efficient storage and retrieval system of Cloud-Based Storage Services can also be mainly referred to as the main reason for its growth in popularity, however the issue of security is still regarded as a major concern resulting in minimal use of Cloud-Based Storage Services. Securing those shares is paramount; for instance, a Dropbox user sharing content in the cloud has no encryption; a hacker can gain access. This research presents the new security concept that incorporates the Caesar cipher algorithm, which is a simple yet efficient substitution cipher to enhance the data security and sanity in cloud storage. In addition it uses a two factor authentication system to ensure that the user is authenticated before accessing link files. This combined method should help decrease the possibility of the unauthorized access and resource-exhaustion attacks. The paper also presents works related to the task, explains the developed security mechanism based on Caesar cipher with double authentication, and evaluates it.

### 1.1 PROBLEM STATEMENT

Critics have noted that cloud-based storage service is more convenient as well as cheaper when compared to other kinds of storage; nonetheless, available studies reveal that such service mediums are highly insecure. Consumers risks includes; Interception risk in the process of file sharing, Resource utilization attack for instance where an attacker sends request to a cloud resource until the resource is paralyzed and made inaccessible to other users. Contemporary approaches to information security such as encryption and users' access rights may be too limited to address all these risks properly. Therefore, there is a need to ensure has well fit methods in order to prevent access from outside parties and to ensure that cloud storage is safe from such disturbances in the same instance ensuring that data is safe.

### 1.2. LITERATURE SURVEY

Alexandros Bakas and Antonis Michalas describes the use of SSE for data indexing followed by secure retrieval under Private Information Retrieval (PIR) and the use of ABE for the purpose of protecting sensitive data will be explained in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, November 2024

this paper. The scheme has a revocation mechanism based on SGX which works independently of the ABE system. This approach has been designed to renew a stronger data protection as well as smart data management for storing data in the cloud[1].

Amos Beimel explores two essential cryptographic tools: The generalized secret sharing schemes and the key distribution schemes are the major categories of secret sharing. In secret sharing schemes, only permitted groups are able to reconstruct the secret which assist in safe storage of secrets and more network operations. These are for the case of larger groups or threshold schemes and the general cases of any monotone collections. LM-variant distribution schemes make it possible for subsets to derive individual keys for the private cryptosystems and authentication. Thus, the tools examined in this thesis are critical to protecting network operations from malicious users[2].

In their work, UA Butt et al. analyze several threats related to cloud computing; the identified types include data breach, insider attack, DDoS attack, and virtualization, insecure API. They describe the effects of these threats and also cloud security measures such as encryption, access control, and network security protocols, policies to reduce risk on clouds[3].

In this context, M Farsi et al. have categorised data security threats in cloud computing in a exhaustive manner. They include unauthorized access and data compromises, malware/virus, DoS attacks, insiders, and APIs and interfaces. This paper seeks to examine how these threats can affect the cloud based systems' integrity, availability, and confidentiality and how these risks can be managed efficiently[4].

In the papers by John Bethencourt, Amit Sahai, and Brent Waters, it is said that the CP- ABE allows to accomplish the access control in the encrypted data without using the trusted servers. It means data confidentiality even in the case of server compromise, and collusion is very much resistant. Unlike other methods, the CP-ABE assigns the access policies to the ciphertexts themselves, not the encrypted data that were placed into the user keys, which conforms to the roles of RBAC. The authors of the system also present an implementation of the system as well as the performance measures[5].

In their paper, Jianting Ning, Xinyi Huang, et al. , focuses on the issue of secure cloud- based data sharing and comes up with two schemes: two dual access control systems that are safe from DDoS/EDoS attacks. They also stress the reusability of their devised download request control technique to other forms of Ciphertext-Policy Attribute- Based Encryption (CP-ABE). In their experiments, they show that the prospective systems need a negligible amount of computations and communication compared to the basic CP-ABE framework[6].

In this paper, Manoj Kumar Sasubilli and Venkateswarlu R refer to the severe security issues concerning cloud computing, with the focus on confidentiality and trust breaches. It emphasizes an organization's requirement to develop sound measures as threats continue to change, stressing on the importance of risk mitigation and prevention of possible assaults[7].

## II. METHODOLOGY

### 2.1 EXISTING SYSTEM

As elaborated in the present context, in the current system, data owners have to come up with a set of challenge ciphertexts to strengthen their defense against possible attacks and increase the computational burden. Further, data users have to decrypt one among these challenge ciphertexts as an additional measure which consumes a lot of computations. Various threats that have been associated with data security in outsourced data remain a major issue that acts as a constrain in the acceptance of the cloud-based storage service.

### 2.2 PROPOSED SYSTEM

The integration of the proposed system provides the dual access control to the data of users using CP-ABE for improved security in cloud with policy based access control. It removes the challenge ciphertexts, and the verification process is done online to the cloud server through any trusted third party. This makes the data confidential and the owner unknown while it allows orderly and controlled request for downloads. Thus, our system reduces the impact of EDoS threats, thereby increasing the general security and dependable use of cloud databases.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, November 2024

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE) conceived to enable a great control over the access to the encrypted data. In CP-ABE systems, the secret key issued to each user depends on the attributes that are assigned to the user. This is based on a planned access structure A that a data owner lays down and which they use to encrypt their data. The usage of linear secret-sharing schemes that have been recently incorporated into CP-ABE systems is normally efficient for this purpose.

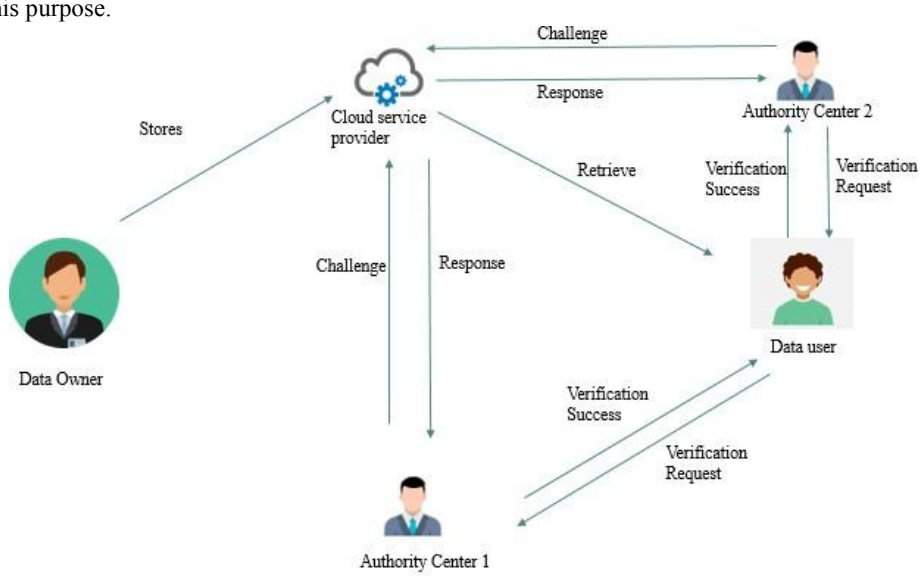


Figure 1 . System Architecture

The system architecture comprises several key roles:

• Authority Center-1: collecting system parameters and registering users; in the first offered setting, the Authority Center-1 receives initial call requests from the cloud.

• Data owners have data which needs to be stored on the cloud, but they do not want just anyone to have access to that data, say only professors or associate professors. Owners are detached when the data is uploaded.

• The data users want to download and decrypt the encrypted files that are kept in the clouds and to which only the users who also have Download and Decrypt permission can have an access.

• The Cloud provides storage solutions which include preserving the outsourced data and dealing with requests for downloads from the data users. Also, for the second system, an

• Authority Center-2 handles calls by processing the call requests originating from the cloud. In the workflow of the current study, the data owners are required to encrypt their data under the chosen access policies and then upload them in to the cloud; the authorized users are then required to download the data through a request to the cloud.

The workflow begins with data owner encrypting his data, using the policy of his choice and then upload the encrypted data in the cloud storage. Once secured, the restricted data consumers can download and obtain the encrypted data by sending download requisites to the cloud service. This procedure makes certain that only individuals, prescribed by the system admin, with the right user ID and password, can decipher the data and use it thereby enhancing the robustness of a system from unauthorized user's intrusion at the time of storage and or during retrieval of the data.

## III. RESULTS AND DISCUSSIONS

In the earlier version of the SecureCloud system, data owners directly come into the case by encrypting their files with their specific and unique policies, then these files are uploaded to the cloud. The end users can then decipher the given files in the cloud infrastructure via download requests since the end users are the only ones authorized to operate on the files. It also make use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to make certain files decryptable only by users with accompanied attributes. From the implementation it became apparent that in regard to the amount of time it took to perform the encryption and decryption functions the complexity was in fact low.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, November 2024

The formulation of assessment for security backed up the protection against entry of unauthorized individuals as well as supporting Internal Threats hence backing up the guarding of the data. Regarding the discussions, the participants directed their attention to the extent and manner in which it dealt with the security and access aspects as well as with the prospects and potential scalability of the system and existence of potential future research themes for cloud security. Thus, SecureCloud can be regarded as an improvement as to the cloud security that encompasses a high form of encryption along with efficient access control mechanisms.

## IV. CONCLUSION

Accordingly, SecureCloud can be referred to as the one that positively enhances the processes of developing the proper approaches to providing for the steady issues of keeping data in cloud computing. By applying these contemporary techniques such as the Ciphertext-Policy Attribute-Based Encryption (CP-ABE), coupled with flexible and potent source of access control methods, the files which are stored in SecureCloud will be rather difficult to be accessed or to be penetrated by people who are unauthorized or accessed by hackers or people with undesirable motives of violating the files. In this system, data owners gain the capability to encrypt a certain file depending on the given access policy; the receivers who possess the access keys that can decrypt the information are those with attributes similar to the access keys. It not only enhances the safety of the data that is being stored but also reduces the danger of employees or insiders or data breach by the workers of the certain organization.

Based on the efficiency of the encryption and decryption in the schemes of SecureCloud system besides performance and computational complexity of the system it can be mentioned that the work is quite well managed and follow the promptness. Therefore, through the incorporation of the two layers, data is more secure and faith in the cloud storage as well as sharing services developed.

Further evolution of SecureCloud may be intended in enhancing the identified threat algorithms and constant monitoring of new threats. Continuing the work with the special modules combined with the practical tasks will continue improving the process of the system's work and to address other advancing features of the cloud computing. The policy of the constant enhancement of security measures and threats counteraction, SecureCloud's goal is to become one of the leading providers of secure cloud data storage for enterprises and for ordinary users with easy expandable and resistant security systems.

## REFERENCES

[1] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.

[2] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[3] Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami,N. (2023). Cloud security threats and solutions: A survey. Wireless Personal Communications, 128(1), 387-413.

[4] Farsi, M., Ali, M., Shah, R. A., Wagan, A. A., & Kharabsheh, R. (2020). Cloud computing and data security threats taxonomy: A review. Journal of Intelligent & Fuzzy Systems, 38(3), 2517-2527.

[5] John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

[6] Ning, J., Huang, X., Susilo, W., Liang, K., Liu, X., & Zhang, Y. (2020). Dual access control for cloud-based data storage and sharing. IEEE Transactions on Dependable and Secure Computing, 19(2), 1036-1048.

[7] Sasubilli, M. K., & Venkateswarlu, R. (2021, January). Cloud computing security challenges, threats and vulnerabilities. In 2021 6th international conference on inventive computation technologies (ICICT) (pp. 476-480). IEEE.