International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Dual Access Control for Cloud-Based Data Sharing and Storage Security

Ramesh Byali [b], *Jyothi* [c], *Megha Chidambar Shekadar* [d]

[b]*cse dept PDIT Hospet India ramesh.byali@gmail.com*
[c]*cse dept PDIT Hospet India*
[d]*cse dept PDIT Hospet India*

DOI: https://doi.org/10.55248/gengpi.2022.3.8.4

ABSTRACT

Abstract—Due to its effective and affordable management, cloud-based data storage has recently attracted growing interest from both academia and industry. Since services are delivered over an open network, it is critical for service providers to adopt secure data storage and sharing mechanisms to protect user privacy and the confidentiality of data. The most popular technique for preventing the compromise of sensitive data is encryption. The actual necessity for data management, however, cannot be fully met by merely encrypting data (for instance, using AES). Additionally, a strong access control over download requests must be taken into account to prevent Economic Denial of Sustainability (EDoS) assaults from being performed to prevent users from using the service. In this essay.In the context of cloud-based storage, we take into account dual access control in the sense that we create a control mechanism over both data access and download requests without sacrificing security and effectiveness. This paper presents the design of two dual access control systems, one for each intended environment. There is also a presentation of the systems' experimental and security analysis. Security Dual Access Control for Data Sharing and Storage in the Cloud

Keywords:Rescue bag, Rescue techniques, Borewell rescue, Child safety

1. Introduction

Due to its extensive list of advantages, which includes access freedom and the lack of local data management, in many Internet-based commercial products (such as Apple iCould). Nowadays, a growing number of people and businesses prefer to outsource their data to faraway clouds in order to avoid having to upgrade their local data management facilities or devices. However, one of the biggest barriers preventing Internet users from embracing cloud-based storage services generally may be their concern about security breaches involving outsourced data. Outsourced data may need to be subsequently shared with others in many practical scenarios. Alice, a Dropbox user, might send her friends pictures.Without employing data encryption, Alice must first create a sharing link and then distribute it to others in order to share the images. The sharing link may be exposed at the Dropbox administration level, even though it guarantees some level of access restriction over unauthorized users (for example, those who are not Alice's friends) (e.g., administrator could reach the link).

A simple solution to prevent shared photos from being accessed by system "insiders" is to specify the group of authorized data users before encrypting the data. However, Alice might not always be aware of who will be receiving or using the photos. Alice might only be aware of attributes related to photo receivers. Here, conventional public key encryption is used (e.g., Paillier Encryption),That cannot be used since it requires the encryptor to know who the data recipient is beforehand. It is therefore desirable to provide a policy-based encryption method over the outsourced photographs, such that Alice may use the mechanism to set access policies over the encrypted photos to ensure that only a select group of authorized people can access the photos.

A frequent exploit known as a resource-exhaustion attack exists in cloud-based storage services. A malicious service user may launch denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks to consume the resources of the cloud storage service server in order to disrupt the cloud service

* *Corresponding author.*
E-mail address: *shahida@pdit.ac.in*

because a (public) cloud may not have any control over download requests (i.e., a service user may send an unlimited number of download requests to the cloud server).Could not fulfill the service needs of sincere customers. Due to increased resource demand, the "pay-as-you-go" model runs the risk of upsetting the economy. Users of cloud services will experience a sharp increase in costs as the attacks intensify. This is referred to as an Economic Denial of Sustainability (EDoS) assault [32, 33], which attacks the financial resources of cloud adopters. Beyond monetary loss, unrestricted downloads itself could provide network attackers access to encrypted download data, which could result in some potential information leaking (e.g., file size). As a result, it is also necessary to have an effective control on download requests for external (encrypted) data.

2. LITERATURE SURVEY

By showcasing two effective and safe cloud-based dual access control systems1 in various scenarios, we answer the aforementioned issue in the positive. We briefly outline the technical road map below with the intention of offering an effective dual access control method. We begin with a CP-ABE system [36], which is viewed as one of the building blocks, to ensure the confidentiality of outsourced data without sacrificing policy-based access control. On top of the CP-ABE system, we also apply an efficient control over data consumers' download requests. We come up with a fresh strategy to do away with the practice of "testing" encrypted text. We specifically enable the creation of download requests by data users. Upon receiving the download request, with assistance from the enclave or the authority,A cloud server called Intel SGX is able to determine whether a user of the data is permitted to view it. The cloud server just learns whether the user is authorized; no other information is disclosed. On the basis of the aforementioned process, the cloud keeps control of the download request. The systems we suggest have the following distinctive characteristics:

(1) Data privacy when it is outsourced. The outsourced data is encrypted in our suggested systems before being uploaded to the cloud. Without authorized access, nobody can access them.

(2) Data sharing anonymity. Given an outsourced data, a cloud server cannot determine the data owner, guaranteeing the owner's anonymity in data exchange and storage.

(3) Strict access control for data that has been outsourced and/or encrypted. After the data is uploaded to the cloud, the data owner still maintains access control over his encrypted data. In particular, a data owner can encrypt the data that was outsourced under a defined access policy so that only a select number of authorized users who comply with the access policy may access the data.

(4) Command over the resistance to EDoS assaults and anonymous download requests. Any system user may send a download request, but a cloud server has control over it and can set the request to be anonymous. We claim that our systems are protected against EDoS attacks thanks to the management over download requests.

(5) Extremely effective. The CP-ABE system is the foundation for our suggested systems [36]. When compared to [36],

3. ARCHITECTURE

Given the security presumption of each of the aforementioned entities, the following are the primary design objectives of our suggested systems:

exchange of anonymous data. The data owner's identity shouldn't be made public. Particularly for recently uploaded files, the cloud is unable to determine the true identity of the file's owner the secrecy of shared data.

- The data that has been outsourced to the cloud should not be visible to authorized or unauthorized users of the data.
- Requests for anonymous downloads.
- Access control while requesting a download.
- EDoS attacks from malevolent data users; only those with permission are able to get shared data from the cloud control over access to shared data.

- Only those who are authorized can decrypt the shared data. Based on the security design and assumptions

4. METHODOLOGY

To protect the data, we use a hybrid system, which combines the effectiveness of symmetric-key systems with the practicality of public-key systems. Particularly, the Key/Data Encapsulation Mechanism (KEM/DEM) option is used for both of the proposed dual access control systems [31]. An effective symmetric-key encryption strategy is used to encrypt the message, as opposed to the ineffective public-key scheme (CP-ABE), which solely employed to encrypt and decrypt a brief key value.We use the following methods to meet the security criteria of anonymous data sharing, data confidentiality, and access control on shared data:CP-ABE technique as the fundamental cornerstone. Because of its effectiveness, we specifically present the construction based on the CP-ABE scheme in [36]. and sophisticated design.

5.CONCLUSION

We presented the idea of SE-EPOM and defined its security definitions in this work.We then used our unique subset choice method to create an actual SE-EPOM scheme in a distributed architecture, and we demonstrated that it satisfies our suggested security requirements. The system also has appealing characteristics like multi-keyword search support, constant size trapdoor and cipher text, hidingEnabling the multi-writer/multi-reader setting, changing the search pattern and access pattern while searching. Lastly, the comparison evaluation methods and ours demonstrates that our distributed SEEPOM scheme beats competing alternatives in terms of total performance. We showed two dual access control systems and addressed an intriguing and pervasive issue with cloud-based data sharing. The DDoS/EDoS assaults can't take use of the proposed systems

REFERENCES

[1] Dr. C.N. Sakhale, D.M. Mate, Subhasis Saha, Tomar Dharmpal, Pranjit Kar, Arindam Sarkar, Rupam Choudhury, Shahil Kumar , "An Approach to Design of Child Saver Machine for Child Trapped in Borehole ", International Journal of Research in Mechanical Engineering, October-December, 2013, pp. 26-38.

[2] K. Saran, S. Vignesh, Marlon Jones Louis have discussed about the project is to design and construct a "Bore-well rescue robot" (i.e. to rescue a trapped baby from bore well), International Journal of Research in Aeronautical and Mechanical Engineering, Boar well rescue robot , pp. 20-30 April 2014

[3] G. Nithin, G. Gowtham, G. Venkatachalam and S. Narayanan, School of Mechanical Building Sciences, VIT University, India, Design and Simulation of Bore well rescue robot– Advanced, ARPN Journal of Engineering and Applied Sciences, pp. MAY 2014.

[4] Camera - Direct web search on google.com

[5] J. Burke and R.R.Murphy, "Human-robot interaction in USAR technical search: Two heads are better than one,"inProc.IEEE Int. Workshop ROMAN, Kurashiki, Japan, 2004, pp. 307-312.

[6] J. Casper and R. R. Murphy, "Human-robot interactions during the robot assisted urban search and rescue response at the world trade center," IEEE Trans. Syst., Man, Cybern. B, Cybern., Vol. 33, no. 3, pp. 367–385, Jun. 2013.

[7] R. R. Murphy, "Activities of the rescue robots at the World Trade Center from 11–21 September 2001," in Proc. IEEE Robot. Autom. Mag., 2004, pp. 50–61.

[8] Rodriguez, K. M., Reddy, R. S., Barreiros, A. Q., & Zehtab, M. (2012, June). Optimizing Program Operations: Creating a Web-Based Application to Assign and Monitor Patient Outcomes, Educator Productivity and Service Reimbursement. In DIABETES (Vol. 61, pp. A631-A631). 1701 N BEAUREGARD ST, ALEXANDRIA, VA 22311-1717 USA: AMER DIABETES ASSOC.

[9] Kwon, D., Reddy, R., & Reis, I. M. (2021). ABCMETAapp: R shiny application for simulation-based estimation of mean and standard deviation for meta-analysis via approximate Bayesian computation. Research synthesis methods, 12(6), 842–848. https://doi.org/10.1002/jrsm.1505

[10] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Usability Evaluation of an Unpopular Restaurant Recommender Web Application Zomato. Asian Journal of Research in Computer Science, 13(4), 12-33.

[11] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Analysis of the Unexplored Security Issues Common to All Types of NoSQL Databases. Asian Journal of Research in Computer Science, 14(1), 1-12.

[12] Singh, P., Williams, K., Jonnalagadda, R., Gogineni, A., &; Reddy, R. R. (2022). International students: What's missing and what matters. Open Journal of Social Sciences, 10(02),

[13] Jonnalagadda, R., Singh, P., Gogineni, A., Reddy, R. R., & Reddy, H. B. (2022). Developing, implementing and evaluating training for online graduate teaching assistants based on Addie Model. Asian Journal of Education and Social Studies, 1-10.

[14] Sarmiento, J. M., Gogineni, A., Bernstein, J. N., Lee, C., Lineen, E. B., Pust, G. D., & Byers, P. M. (2020).Alcohol/illicit substance use in fatal motorcycle crashes. Journal of surgical research, 256, 243-250.

[15] Brown, M. E., Rizzuto, T., & Singh, P. (2019). Strategic compatibility, collaboration and collective impact for community change. Leadership & Organization Development Journal.

[16]Sprague-Jones, J., Singh, P., Rousseau, M., Counts, J., & Firman, C. (2020). The Protective Factors Survey: Establishing validity and reliability of a self-report measure of protective factors against child maltreatment. Children and Youth Services Review, 111, 104868.

[17] Reddy Sadashiva Reddy, R., Reis, I. M., & Kwon, D. (2020). ABCMETAapp: R Shiny Application for Simulation-based Estimation of Mean and Standard Deviation for Meta-analysis via Approximate Bayesian Computation (ABC). *arXiv e-prints*, arXiv-2004.