Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 10, October 2019

Secure And Expressive Cloud Storage Data Access Control for Data Security

[1]Mirza Moiz Baig,[2]Umesh Samarth,[3]Shivani Nilewar,[4]Birpal Singh Kapoor

[12]Assistant Professor,[34]Student
Department Of Information Technology
J D College of Engineering & Management, Nagpur

ABSTRACT

In order to ensure the classification of reappropriated information while also providing adaptable information access to cloud clients whose information is not under their physical control, secure distributed storage is a growing cloud administration trend. One of the most promising methods for verifying the administration's certification is cypher text-policy attribute-based encryption (CP-ABE). Due to the inherent "win big or bust" unscrambling feature of CP-ABE, the adoption of CP-ABE may result in an inescapable security breach known as the abuse of access accreditation (for example, decoding privileges). Here, we focus on two key cases in which a cloud client's access qualification is abused by a semi-believed specialist. CryptCloud+, a distributed storage platform with white-box discernibility and review, is proposed as a way to limit the exploitation of the system. Additionally, we demonstrate the framework's usefulness by conducting studies.

1.INTRODUCTION

Cloud processing is the critical parts of PC world. It empowers adaptable, on-request, and ease of figuring assets. In any case, the data is outsourced to some cloud servers, and different protection concerns rise up out of it. The one of the basic services of cloud processing is the putting away limit of cloud which empowers clients (data proprietor) to have their data in cloud by methods for cloud server. It gives the data access to data shoppers. It can likewise give on request assets to storage which can help specialist organizations to lessen their support costs [1]. Ordinarily clients store his/her data in confided in servers. These data are controlled by a trustable chairman [2]. The cloud storage can gives the authorization to clients to get to their data from anyplace on any gadget in proficient way. The client's secret key is put away in their PC [10]. In cloud registering there are a few outlines is proposed to secure the cloud storage. The attribute based encryption approach is the one among sorts of encryption framework [6]. In this sort of framework, every client has the client secret key is issued by the authority. This encryption strategy is the effective adaptable approach which executes attribute-based access control (ABAC) by utilizing data or subjects' attributes as data get to strategies and also public keys [10]. AttributeBased Encryption (ABE) is a promising methodology for cloud storage that offers finegrained get to control approach over encoded data [2]. Attribute-based Encryption (ABE) is viewed as a standout amongst the most reasonable plans to lead data get to control in public clouds for it can ensure data proprietors' immediate control over their data and give a fine-grained get to control benefit. It manages confirmed access on scrambled data in cloud storage benefit [8].There are numerous ABE plans proposed, which can be partitioned into two classes: Key Policy Attribute based Encryption (KP-ABE), Cipher content Policy Attribute-based Encryption (CPABE) [2]. In the KP-ABE, a figure content is related with an arrangement of attributes, and a private key is related with a monotonic access structure [3] [1]. Contrasted and KP-ABE, CP-ABE is a favored decision for planning access control for public cloud storage. The CPABE is utilized for data proprietors and based on get to arrangements, to give adaptable, fine-grained and secure access control for cloud storage frameworks [3]. In CPABE plot, there is an authority that is in charge of attribute administration and key appropriation. There are two sorts of CP-ABE frameworks: single-authority CP-ABE where all attributes are overseen by a solitary authority, and multiauthority CP-ABE [4]. CP-ABE is utilized to data get to control for cloud storage, some multiauthority CP-ABE plans, has

proposed. Exceptionally, in DAC-MACS [1], other than proposing a multi authority CP-ABE plot for cloud storage, the creators asserted that the attribute renouncement component [5]. The client's entrance authorization relies upon the attributes the client holds in the CP-ABE based access control framework, and each attribute might be controlled by numerous data clients [7]. CP-ABE plot was proposed to totally conceal the entrance strategy. In any case, the plan just bolstered the straightforward 'AND' door get to structure [9].In request to enhance the framework security, ensure client protection and spare the storage overhead of figure content, for cloud storage [8].

2.LITERATURE SURVEY

2.1 Mobile cloud computing: A survey

AUTHORS: N. Fernando, S. W. Loke, and W. Rahayu

Despite increasing usage of mobile computing, exploiting its full potential is difficult due to its inherent problems such as resource scarcity, frequent disconnections, and mobility. Mobile cloud computing can address these problems by executing mobile applications on resource providers external to the mobile device. In this paper, we provide an extensive survey of mobile cloud computing research, while highlighting the specific concerns in mobile cloud computing. We present a taxonomy based on the key issues in this area, and discuss the different approaches taken to tackle these issues. We conclude the paper with a critical analysis of challenges that have not yet been fully met, and highlight directions for future work.

2.2 Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges

AUTHORS: S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya
Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. CMA is the state-of-the-art mobile augmentation model that employs resource-rich clouds to increase, enhance, and optimize computing capabilities of mobile devices aiming at execution of resource-intensive mobile applications. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. Researchers utilize varied cloud-based computing resources (e.g., distant clouds and nearby mobile nodes) to meet various computing requirements of mobile users. However, employing cloud-based computing resources is not a straightforward panacea. Comprehending critical factors (e.g., current state of mobile client and remote resources) that impact on augmentation process and optimum selection of cloud-based resource types are some challenges that hinder CMA adaptability. This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. We critically analyze the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present a taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions.

2.3Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems

AUTHORS: R. Kumar and S. Rajalakshmi
The concepts of Cloud computing are naturally meshed with mobile devices to enable on-the-go functionalities and benefits. The mobile cloud computing is emerging as one of the most important

branches of cloud computing and it is expected to expand the mobile ecosystems. As more mobile devices enter the market and evolve, certainly security issues will grow as well. Also, enormous growth in the variety of devices connected to the Internet will further drive security needs. Understanding the true potential of mobile cloud computing and identifying issues with mobile cloud security, privacy, feasibility and accessibility remain a major concern for both the customers and the enterprises. This paper covers the mobile cloud security issues and challenges by looking at the current state of cloud security breaches, vulnerabilities of mobile cloud devices, and how to address those vulnerabilities in future work in aspect of mobile device management and mobile data protection. Also, it highlights on usage of SCWS (Smart Card Web Services) rivalry to intensify security of mobile cloud computing.

2.4 Mobile cloud sensing, big data, and 5g networks make an intelligent and smart world
AUTHORS: Q. Han, S. Liang, and H. Zhang
Through time, we have seen mobile phones transform into multifaceted devices, adapted to meet and exceed our everyday needs. These needs range from something as personal as a health care manager to something as purely analytical as an environment monitor. In effect, mobile phones have come into our lives, making life easier, smarter, and more efficient. In this article we discuss mobile sensing and cloud computing separately and in detail, then combine the two concepts to form the singular idea of mobile cloud sensing. We will also give an intuitive architectural description of mobile cloud sensing, along with discussions about each of its individual building blocks. There are limitations to mobile cloud sensing today, but with the emergence of 5G coupled with the analysis of big data, we can address the current issues at hand. We believe that with the advent of mobile cloud sensing, 5G, and big data analysis, our lives will continue to see an increase in overall quality.

3.PROPOSED SYSTEM
An accountable authority and revocable Crypt Cloud+ (referred to as Crypt Cloud+) has been designed to address the issue of credential leakage in CP-ABE based cloud storage systems. White-box traceability, accountable authority, auditing, and effective revocation are all supported together for the first time in a cloud storage system built on the CP-ABE protocol with this technology. Our ability to track down and ban rogue cloud users is greatly enhanced by Crypt Cloud+ (leaking credentials). When the semi-trusted authority redistributes the user's credentials, our approach can also be used.

3.1 IMPLEMENTATION

1. Data owner:
Is an entity who encrypts its documents under an arbitrary access control policy and outsources them to the cloud. He/She considers the time of encrypting in generating the cipher texts. We should highlight that the data owner also encrypts his/her documents under his/her arbitrary access control policy. However, in this paper we concentrate on the encryption of the extracted keywords from documents.

2. **Data user:**
Is an entity who is looking for documents which contains an intended keyword, and are encrypted in a determined time interval. The time interval is arbitrarily selected by the data user.

3. **Cloud Server :**
Is an entity with powerful computation and storage resources. CS stores a massive amount of encrypted data, and owner will monitor all file detaills

4. **TPA**
In this TPA will login by using valid user name and password after login tpa will give permission to user for login and then TPA will trace data and provide results to data owner.

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 10, October 2019

5. STA

In this module STA login by using valid user name and password after STA will provide permission to user for data access.

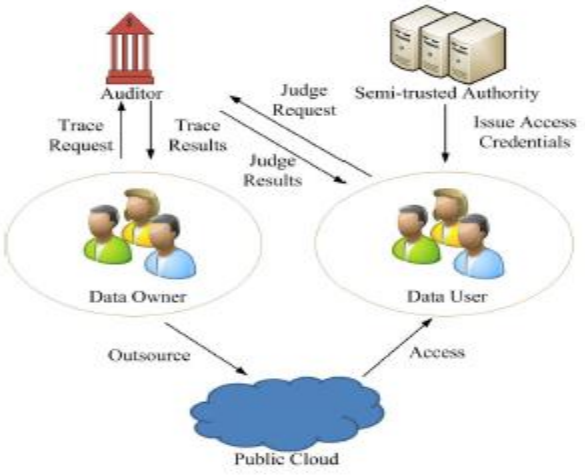

Fig 1: Architecture

4. RESULTS AND DISCUSSION

Fig 2: Home Page of Crypt cloud

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 10, October 2019

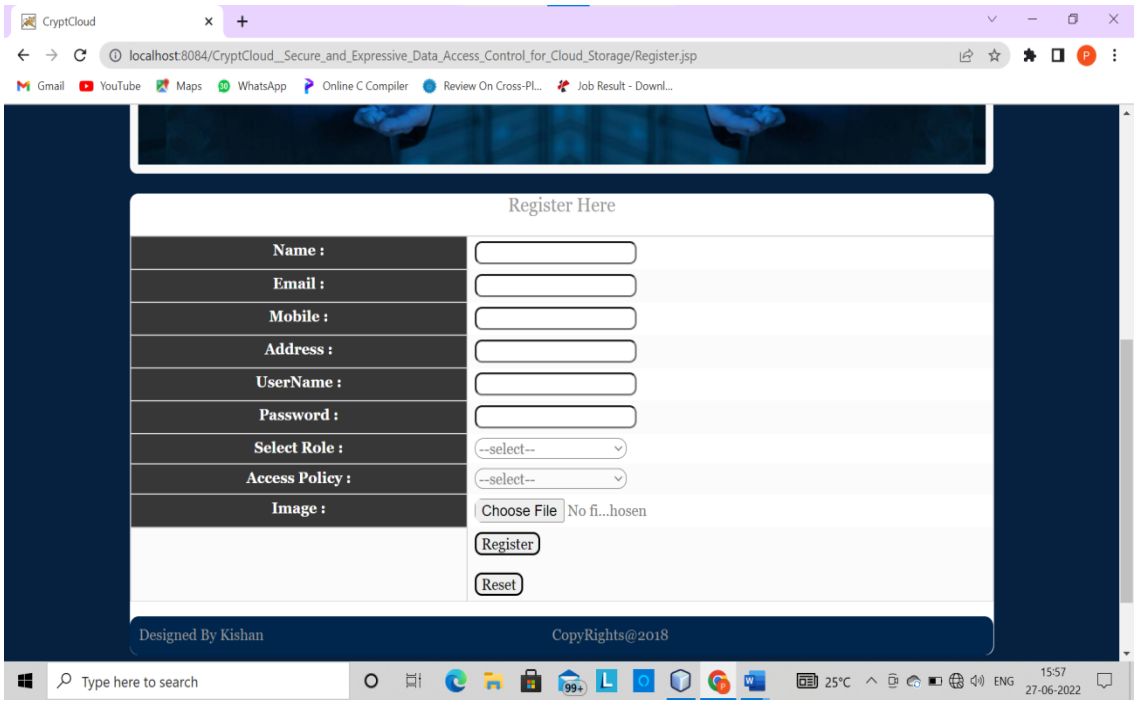

Fig 3: Showing the data user's registration page

Fig 4: Data user's home page after login of data user

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 10, October 2019

Fig 5: Data owner's home page after login of data owner

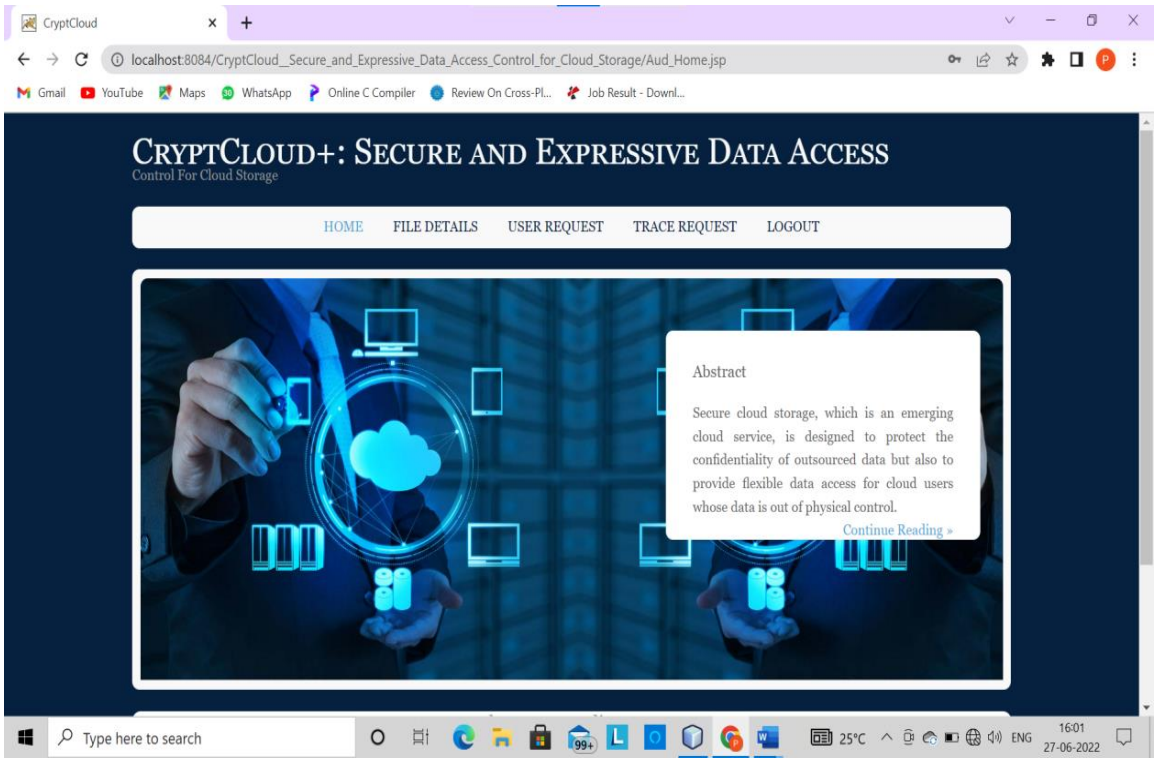

Fig 6: Auditor's home page after login of auditor

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 10, October 2019

Fig 7: Cloud's home page after login of cloud

Fig 8: STA's home page after login of STA

5.CONCLUSION

CryptCloud+, a responsible expert and revocable CryptCloud that provides white-box discernibility and examination, has been used in this work to verify certification spillage in CP/ABE based distributed storage frameworks. First CP-ABE based distributed storage architecture that provides white-box detection, responsible expert, inspection and successful repudiation all at the same time The CryptCloud+ feature, in example, enables us to track and block spiteful cloud customers (spilling

accreditations). Our solution can also be used in the case where the semi-confided in power redistribute the qualifications of the clients. As a more grounded concept (as opposed to white-box recognizability), we believe that in Crypt Cloud, we may require discovery detect ability. One of our upcoming projects will be to consider and examine the finding detect capabilities.

REFERENCES

[1] Kaiping Xue" RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage", IEEE2016.
[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.
[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.
[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.
[5] Y. Wu, Z. Wei, and H. Deng, "Attribute based access to scalable media in cloud assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.
[6] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271– 2282, 2013.
[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.
[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on time sensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.
[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.
[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology– EUROCRYPT 2011. Springer, 2011, pp. 568–588