International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Novel Framework for Encrypted Data Access Control in Cloud

Prof. GOWRISHANKAR[1], KRITHIKA M[2]

[1]*Dept of CSE, BMS College of Engineering, Bangalore.*
[2]*M.Tech Student, Dept of CSE, BMS College Of Engineering, Bangalore.*

Abstract*: Data access control becomes a problem in the cloud storage talk to prevent unauthorized data use, proper access control is required for the multi-user system. In File Sharing System, as Multiple Owners in File Sharing Program, Like Many Owners In this paper, we have developed a clear and effective database management system for multi-cloud storage, where multiple authorities and each authority are able to execute attributes independently. Specifically, we propose a multi-jurisdictional system, and use it as a sub-standard for designing a data access control system. The analytical and simulation results show that the proposed system is more accessible than the previous works.*

INTRODUCTION

With the development of a new computer paradigm, cloud computing [1] is becoming increasingly important, providing easy, on-demand services from a shared pool of computational computing resources. Thus, a growing number of companies and individuals are choosing to outsource their data storage to the cloud server. Despite the great economic and technological benefits, unsafe concerns and privacy issues [2], [3] are becoming the most prominent issue that prevents widespread coverage. Adoption of data storage in public cloud infrastructure. Encryption is a basic way to protect data privacy in remote storage [4]. However, how to get rid of it successfully

Searching for a clear keyword becomes difficult for encrypted data due to the cipher text's inaccessibility. Encryption is searchable that provides a way to allow keyword searches with embedded information [5], [6]. As we may know, leaks of any sensitive student information stored in the cloud can lead to various consequences for the organization and individuals (e.g. litigation, loss of competitive advantage, and criminal charges). Is it possible to revoke the invalid access rights? For example, the security officer of the organization installs a key to teach Alice to an outsider Bob (not a university employee). One possible answer to the question is the use of multiple officers. Besides, this poses an additional cost to networking and infrastructure development, and in the meantime, the problem of strong intergovernmental relations persists. Therefore, we leave that using an authorized reporting method to reduce escrow accessibility problem is the most popular method. We want to minimize legitimate misuse, suggesting Crypto Cloud, the responsive authority and CP-ABE cloud storage system that has tracking and white box testing. To the best of our knowledge, this is the first practical solution to the security of the collected access control of cloud-based data.

Background Work

Encryption searches enable keyword searches with encrypted information. The concept of public key encryption with keyword search (PEKS) has been proposed by Boneh et al [12], which is important for protecting the privacy of exported data. The owners of data in the PEKS schemes [7], [8], [16] keep their forms in a format hidden from a remote data server that is not trusted. Data users want to query on the hidden ry les by generating a keydo trapdoor, and the data server performs a search operation. The water et al. [5] showed that the PEKS scheme can be used to build searchable logs. Later, Xu et al. [17] presented a general framework for combining PEKS with keyword search without concrete. Tang [18] proposed a multidimensional encryption scheme that can be performed along with a pairing scheme. In 2016, Chen et al. [3] introduced the "dual-server" concept in PEKS to resist guessing of a foreign keyword attack. Yang et al. [19] introduced a provisional and time-limited encryption mechanism for a representative on the PEKS system to monitor the deployment of time-controlled authorities. Wang et al. [1] proposed a coded keyword search program for unmatched accessibility, in which order-save symmetric en-cryption was used [35]. Cao et al. [3] designed a novel system to recognize searches for multiple keywords. Readability writing is also studied in [20], [21], [22]. In the context of Attribute-based Encryption (ABE), Sa-hai and Waters [41] originally introduced the concept of ABE, which was subsequently published by Goyal et al. [15]. In particular, Goyal et al. comes with Key-Policy Attribute-based Encryption (KP-ABE) and Cipher textPolicy Attribute-based Encryption (CP-ABE). Since then, a list of ABE strategies has been proposed in the literature [9], [18], [19]. While these programs are designed to achieve improvement, transparency and security, they do not address tracking and dismissal issues. Li et al. introduces a responsive CP-ABE view [23] to prevent unauthorized key distribution among embedded users. In a recent work [22],

a multi-user CP-ABE response plan was proposed. Liu et al. we have also proposed a white box [17] and a black-box [16] protocol for 1 CP-ABE systems that support policy clarity on any monotone access structures. Buildings. Ning et al. [20], propose several effective CP-ABE systems with white box tracking and black box tracking. Deng et al. [11] pro-vide CP-ABE approach to obtain mature access credentials in the cloud storage system.

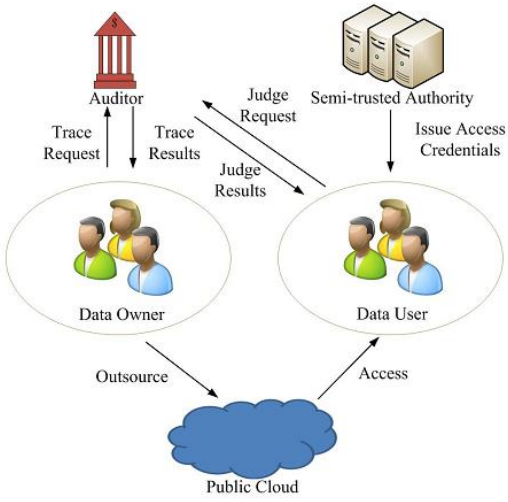

Fig. 1 CP-ABE based cloud storage system

A number of multidisciplinary solutions to CP-ABE systems have also been proposed in the literature, such as. Sahai et al. [22] corrects the problem of duplicate maintenance and provides a completely secure construction of ABE based on the distributed power supply. Yang et al. [24] propose a CP-ABE system for an inaccessible and accessible security back and forth. Recently, Yang et al. [5] propose a method for updating the attribute to achieve a dynamic change in the attribute (such as updating the previous attribute and re-assigning the previously specified attribute). However, the aforementioned studies do not address the mistreatment of key reproductive authorities, the possibility of investigation, and the exclusion (of misconduct). These are the problems we are looking to fix in this paper.

PROPOSED APPROACH

An overview of the methodology we use to detect the presence of malicious cloud users, accountable authority, audits and fraudulent cloud users is listed below (please refer to Sections 7 and 8 for more technical information). As previously discussed, to track malicious cloud users accessibility, we use Paillier-like encryption [38] as an output commitment to achieve white box compliance. Specifically, the commitments that can be issued allow us to create a user ID when we request confidential access. Commitment is considered part of trust. Because of how to hide and bind An overview of how we use traceabil-ities to not exploit the clouds, responsive authority, discriminatory research and depletion of corrupt cloud users is listed below (please refer to sections 7 and 8 for more technical details.) As previously discussed, to track cloud users with high-risk access, we use Pailfer-like encryption [8] as an optional commitment to achieve white-box compliance. Specifically, the commitments that can be issued allow us to create a user ID when we request confidential access. Commitment is considered part of trust. Due to a hiding and binding method of commitment such as the Paillier issue, the user is unable to uncover and continue to "change" the "embedded" identity.

In fact. The Trace algorithm allows us to use the trapdoor commitment to recover the user's identity from the appropriate target. We note that the authentication needs to perform a validation access check (e.g., using the key-key algorithm) before the next step. A check for accessibility for authentication is an algorithm for precision [13], [14], which is used to determine the identity of a well-formed structure within a clay. To reduce commitment, we will not need to keep an identity table, which is not the same as the method presented in [25]. This allows us to "reduce" the additional cost of tracking storage. To achieve responsive authority, accessibility is considered by both the authority and the corresponding user. This prevents the authority from taking full control of the user the user is allowed to access the primary uac (in terms of their identity and identity) from the authority through a secure access protocol. But the administrator does not know what access the user has accessed. If the administrator (reset) distributes the registered user ~ uac (with access to the verified uac) without the user's permission, then all but likely is possible, the uac will differ from the user's uac. The verification access couple (uac; ~ uac) will create subtle evidence of authority misconduct. We note that a similar process can be used to enable an auditor to determine if a user accused of credential leak is guilty. We assume that the auditor must be fair and credible (e.g., an external KPMG or PwC).

REVOCATION MECHANISM

We offer two critical removal methods to recover malicious users completely or completely, inspired by [4], [23]. For transparent decryption, we specify the direct debug list RL directly in the Encrypt algorithm. During the KeyGen algorithm operation, the primary secret key is divided into two parts: one for access control and the other for decryption. For malicious users in RL, they will fail to uninstall any new device as the sub-master secret key

associated with the deletion component cannot be canceled on re-release. With full deployment, Encrypt operations do not need to know the deployment list. Instead, the algorithm Key Update releases a recovery key for all uninsulated users. We use a (random secret) first degree polynomial (i.e., f (w) = w +

) and f (1); f (t) to assign the primary secret key between the private key and the update key, where f (1) is used for access control and f (t) is for deletion. For malicious users in RL, since they cannot access the update keys, they cannot translate any new cipher text. The undo property is obtained by combining the trace and debugging methods described above. In particular, the tracking method ensures that when a user is found to be dangerous (e.g. a leak sure), his or her identity will be listed in the spill. By applying the clear and baseless techniques of destruction we have introduced to the disposal list, we are confident that any "new" text cannot be rewritten by "exiled" users.

Performance Evaluation and Experimental Results

In this section, we evaluate the performance of the proposed systems presented in sections 7 and 8. The tests were performed on a laptop containing the following information: Intel Core i5-5200U, 2.20 GHz, 4 GB memory, and Windows 7 operating system via Service Pack 1. We use a cryptography based pairing library [28] in A1 curve to detect proposed plans. The programming language used is Java with JDK32-1.6.0 and JPBC-2.0.0 [10].

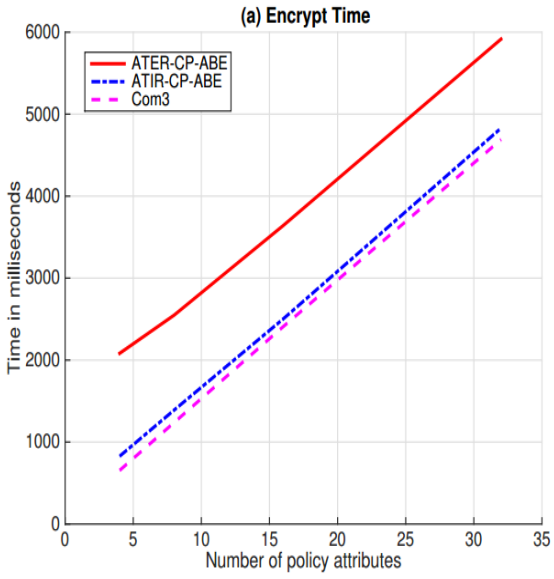

Figure 3a: Encryption Time

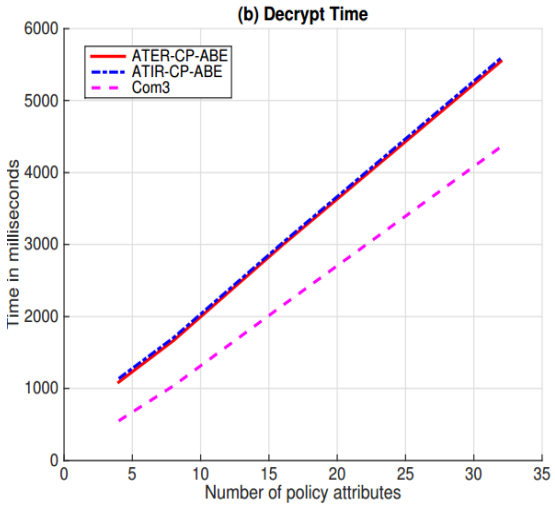

Figure 3b: Decryption Time

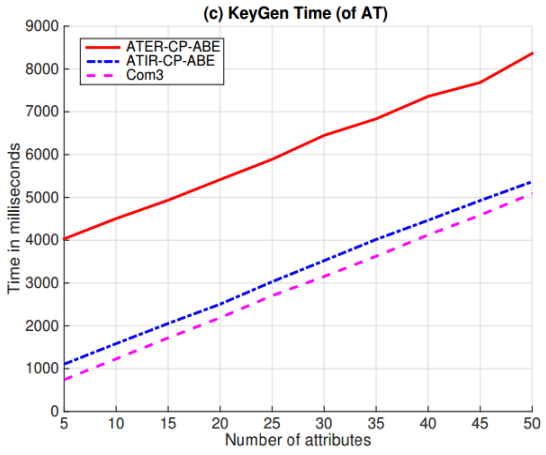

Figure 3c: Key Generation time

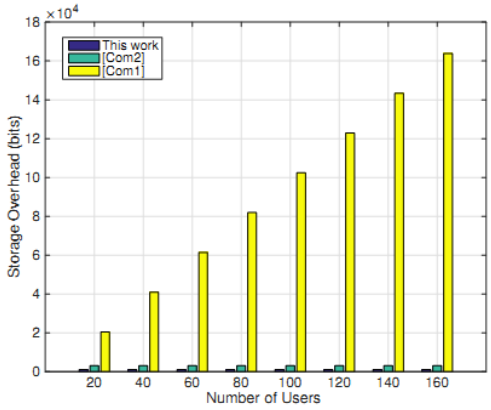

Figure 3c: Key Generation time

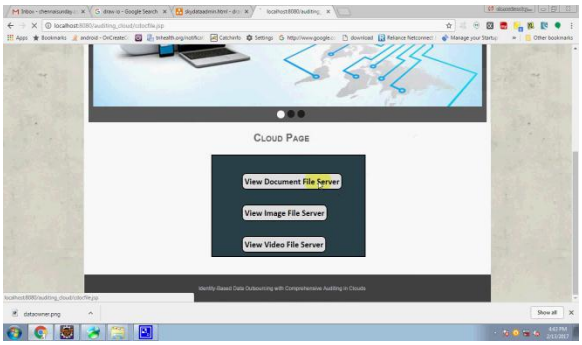

Figure 3: Cloud storage page.

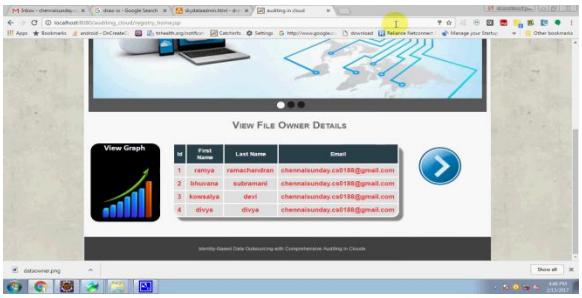

Figure 4: File owner details

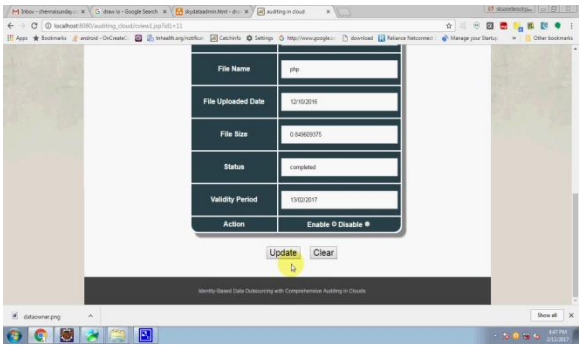

Figure 5: Access permissions update

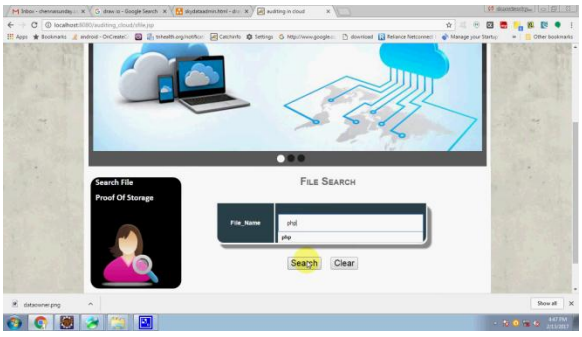

Figure 6: File search at the cloud

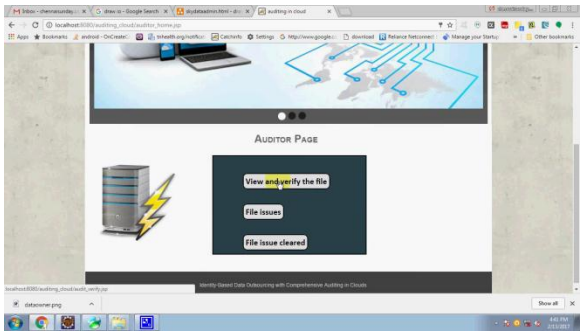

Figure 7: Auditor page

In CP-ABE systems, the complexity of the interrupt policy affects the encryption time and the compile time. In response to this, we generate cipher policies in the form of (S1 and S2 ... and Sl) to simulate the worst case scenario, where Si is a factor.

We attempted to evaluate the efficacy of ATER-CP-ABE and ATIR-CP-ABE by comparing the total time taken for each stage with the actual CP-ABE scheme in [18] (presented as Com3), which does not take into account evidence of abuse of warranties and the issue of withdrawal. As shown in Fig. 3, we look at the time cost of performing each phase (including Encryption Time, Encryption Time and KeyGen Time (for AT)). Given the fact that both of them are reaching for the issue of legitimate abuse and withdrawal, it is not surprising to see that our systems require more time. From Fig. 3 (a), Fig. 3 (b) and Fig. 3 (c), we see that our ATER-CP-ABE and our ATIR-CP-ABE address both the challenges of authenticity and dissolution without introducing greater visibility compared to the actual CP-ABE system in [18]. We note that the approach to the problem of accessibility constraints and the issue of accuracy (as presented in this paper) is a general construct and applies to other CP-ABE systems. In other words, it is possible to apply our technique to a more efficient CP-ABE to improve efficiency.

CONCLUSION

The emphasis on access control and keyword search support are key issues in secure cloud storage. In this work, we outlined a new paradigm for inaccessible encryption, and proposed a concrete architecture that allows us to track and retrieve dangerous cloud users (leaky warranties). Our method can also be used in cases where user credentials are distributed by trusted administrators. We note that we may need black box tracking, which is a strong idea (compared to white box tracking), in the current way. One of our future tasks is to process black box tracking and auditing. In addition, the AU is thought to be completely reliable in the current way.

However, in practice, it may not be the case. Is there a way to reduce trust from the AU? Ideally, one way is to use multiple AUs. This is similar to the strategy used in divination programs. But it will require more communication and distribution costs and in the meantime, the problem of integration between AUs continues. An alternative approach is to use secure hiring of multiple parties in the presence of adversarial opponents. However, it works well and is a bottle. Establishing a multi-party coalition and relying on AU divisions (while maintaining the same level of security and efficiency) is also part of our future work.

REFERENCES

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404,2017.

[2] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patter-son, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4] Nuttapong Attrapadung and Hideki Imai. Attribute-based en-cryption supporting direct/indirect revocation modes. In Cryptog-raphy and Coding, pages 278–300. Springer, 2009.

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

[6] Mihir Bellare and Oded Goldreich. On defining proofs of knowl-edge. In Advances in Cryptology-CRYPTO'92, pages 390–420.Springer, 1993.

[7] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasi-lakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal,4(1):75–87, 2017.

[9] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual systemABE in prime-order groups via predicate encodings. In Advancesin Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing basedcryptography. In ISCC 2011, pages 850–855. IEEE, 2011.

[11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang,and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.

[12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasi-lakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.

[13] Vipul Goyal. Reducing trust in the PKG in identity based cryp-tosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447.Springer, 2007.

[14] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.

[15] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of en-crypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. ACM, 2006.