**SAFE AND PERSUASIVE DATA ACCESS MANAGEMENT FOR SKY STORAGE: CRYPT CLOUD+**

*1MD.Abrar , 2l.Chaithanya ,3*  *N. Sairaml, 4Mrs. G.Gouthami*

# *1,2,3bachelor Degree, Cse,* *Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

*4Mrs S.Gouthami, Associate Professor, bachelor Degree, Cse, Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

**ABSTRACT:**

Secure cloud storage is a newly developed cloud service that is intended to safeguard the privacy of outsourced data while also enabling flexible data access for cloud users whose data is not under their direct physical control. One of the most promising methods that may be used to protect the service guarantee is Cipher text-Policy Attribute-Based Encryption (CP-ABE). However, because CP-ABE has an inherent "all-or-nothing" decryption feature, using it might result in an unavoidable security violation known as the abuse of access credentials (i.e., decryption privileges).

In this article, we look at the two most common instances of access credential misuse: one on the side of the semi-trusted authority and one on the side of the cloud user. The first responsible authority and revocable CP-ABE-based cloud storage system with white-box traceability and auditing, dubbed Crypt Cloud+, is what we suggest as a solution to the problem. Additionally, we provide a security analysis and do additional experiments to show how useful our technology is.

**INTRODUCTION:**

The ubiquity of cloud computing may, inadvertently, expose users' privacy and the confidentiality of their outsourced data. How to ensure that only authorised users may access the data that has been outsourced to the cloud at any time or location is a special difficulty in this situation [3]. One simplistic option is to encrypt the data before transferring it to the cloud. The approach does, however, restrict future data processing and exchange. This is the case due to the fact that a data owner must download encrypted data from a cloud storage service and then re-encrypt it for sharing (assuming the data owner does not have any local copies of the data).

In the realm of cloud computing, a customised control of access over encrypted information can be desirable [51].

Here, Cipher text-Policy Attribute-Based Encrypt (CPABE) [15] could be a good option to ensure data confidentiality and offer granular access control. For instance, in a CP-ABE-based cloud storage system, businesses (such as the University of The United States of America at San Antonio) and people (such as pupils, lecturers, and visitors of the university) can first specify the access policy over the attributes of a potential cloud user. Then, authorised cloud users receive access credentials.

This can be utilised to get access to the data that was outsourced.

In addition to providing a dependable way to safeguard data saved to the cloud, CP-ABE's strong one-to-many encryption technique also makes it possible to implement precise control of access over the data.

In general, the CP-ABE based cloud storage solutions do not take the abuse of access credentials into account. In accordance with some access policies that comply with the pertinent data sharing and privacy laws (such as the USA's Family Educational the Rights and Privacy Act (FERPA) and the Healthcare Portability and Accountability Act of 1992 (HIPAA), for example, a university may deploy a CPABE-based cloud storage system to outsource encrypted student data to the cloud. All users (such as pupils, educators, and visiting scholars) receive login info from the organization's in-charge official when the system settings are initialised and initialised (for example, by the university's security manager).

Each employee is given a variety of titles (such as "administrator," "senior manager," "financial officer," "tenured faculty," "tenure-track faculty," "nontenure-track faculty," "instructors," "adjunct," "visitor," and/or "students") to describe their roles. The student data stored in the cloud (such as student admission files) can only be accessed by personnel who meet the requirements of the decryption policy of the outsourced data.

As we may have known, the disclosure of any personal student data kept in the cloud might have a number of negative effects on the organisation and its members, including legal action, a loss of competitive advantage, and criminal charges. The CP-ABE might assist us in preventing outside intruders from breaching our security.

But how could we definitively prove that an insider of the organisation is guilty of the "crimes" relating to the dispersion of decryption privileges and the circulation of student information in plain format for illegal financial gain? Can you cancel the compromised access credentials for us as well?

We also have a query that has to do with key generation authority in addition to the ones mentioned above. A semi-trusted authority often issues a cloud user's access credential (i.e., decryption key) depending on the qualities the user possesses.

How can we be sure that this specific authority won't give the created access credentials to anybody else? As an illustration, a university employee named Bob receives the lecturer Alice's key from the organisation security officer. Using several authority is one solution to the problem. However, this results in increased communication and infrastructure implementation costs, and the issue of malevolent coordination among authorities continues in the meanwhile. Therefore, we argue that the best course of action for addressing the access credential escrow issue is to use an accountable authority method.

**RELETED WORK:**

Cloud storage investigates new uses for data storage, since the data owner no longer bears entire responsibility for managing data "in local" [43]. However, as data ownership and access are separated in a cloud environment [24], cloud service providers must take over the administration of data, software, physical computers, and platforms, leaving the data owner with limited control over virtual machines [2], [46].

Numerous cloud-based fine-grained access control systems have been introduced in the literature to safeguard the confidentiality of cloud data [1], [20], [21], [25], [44], and [47]. By employing the predefined keywords, searchable encryption allows for secure search across cipher texts [12].

Users can examine the accuracy of the data that has been outsourced [53] and get rid of storage redundancy [48] thanks to data audit and deduplication.

Internet of Things (IoT) and cloud storage are thought to work well together [8, [16], and [54]. This is due to the fact that the cloud may offer significant storage and computational capabilities for IoT devices, which are often resource constrained (e.g., in e-health networks [45], [55], and vehicular DTN network [56]). However, this fusion creates issues with privacy and security.

The concept of attribute-based encryption (ABE) is first introduced in the context of ABE by Sahai and Waters [41], and is subsequently formalised by Goyal et al. [15]. Goyal et al. propose Cipher text-Policy Attribute-Based Authentication (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE) in particular. Numerous ABE systems have since been put out in the literature [9], [18], [19], [31], [37], and [42]. Despite the fact that these methods are intended to increase efficiency, expressiveness, and security, they do not solve difficulties with traceability and revocation.

To stop unapproved key distribution among conspired users, Li et al. present the concept of responsible CP-ABE [23]. A user responsible multi-authority CP-ABE system is suggested in a subsequent paper [22]. White-box [27] and black-box [26] traceability 1 CP-ABE systems providing policy expressions in any monotonous access structures were also presented by Liu et al. Ning et al. [30], [32], [34], and [36] suggest a number of useful CP-ABE systems with both white-box and black-box traceability. A CP-ABE tracing technique is provided by Deng et al. [11] to locate the compromised access credentials in a cloud storage system.

The literature has also put out a variety of attribute cancellation methods for CP-ABE systems, including [52]. Using cipher text delegation, Sanai et al. [40] outline the issue of revocable storage and offer a completely secure structure for ABE. A reversible multi-authority CP-ABE system that accomplishes both forward and backward security is suggested by Yang et al. [49]. Yang et al.'s [50] proposal for an attribute updating technique to enable dynamic attribute modification (such as revoking a prior attribute and re-granting a prior attribute that had been revoked) is more current.

The study works described above, however, do not take into account the misconduct of key generating authority, the viability of auditing, or the revocation (of misbehaver).

These are the issues that this essay aims to answer.

**EXISTING SYSTEM:**

**PROPOSED SYSTEM:**

**RESULT:**

**CONCLUTION :**

In this study, we have developed an accountable authority and revocable Crypt Cloud that allows white-box transparency and auditing (which is referred to as Crypt Cloud+) in order to solve the problem of credential leakage in CP-ABE based cloud-based storage systems. The first cloud storage solution based on CP-ABE to provide white-box traceability, responsible authority, auditing, and effective revocation all at once is this one.

In particular, Crypt Cloud+ gives us the ability to track down and ban rogue cloud users that leak passwords. Our strategy is equally applicable in the scenario when the semi-trusted authority redistributes user credentials.

We point out that black-box traceability, which is a stronger concept (than white-box traceability), may be necessary for Crypt Cloud. One of our upcoming projects will look at black-box audits and traceability.

Furthermore, Crypt Cloud+ presumes that AU can be completely trusted. In actuality, though, it could not be the case.

Is it possible to lessen AU trust in any way? Using different AUs seems to be one approach. This approach is comparable to threshold schemes. However, it will come at an extra expense in terms of deployment and communication, and the issue of AU collusion continues in the meanwhile.

Employing secure multi-party computation in the presence of hostile attackers is another possible strategy. But efficiency also creates a bottleneck. Our future work will also include developing efficient multi-party computation and decentralising trust across AUs while retaining the same degree of security and efficiency.

To accomplish white-box accountability, we employ Parlier-like encryption that serves as an easily extracted promise.

From an abstract perspective, every extractable commitment might theoretically be used to implement white-box traceability. We could utilise a lighter (pairing-suitable) obtainable commitment to increase tracing's efficiency.

Additionally, the primary secret key must be provided as input to the trace algorithms in Crypt Cloud+ in order to provide white-box traceability of malicious cloud users. Evidently, the suggested Crypt Cloud+ is a private, trackable system.

While partial/full public accountability allows the administrator, authorised users, and even anybody without access to the system's secret information to complete the trace, private traceability only permits the system administrator to perform the tracing algorithm. We'll be developing Crypt Cloud+ in the future to offer "partial" and completely public traceability without sacrificing speed.

**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 Patterson, 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 encryption supporting direct/indirect revocation modes. In Cryptography 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 knowledge. 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. Vasilakos. 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 system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. 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 Vasilakos, 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 cryptosystems. 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 encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. ACM, 2006.

[16] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8):2481–2501, 2014.

[17] Allison Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Advances in Cryptology–EUROCRYPT 2012, pages 318–335. Springer, 2012.

[18] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Advances in Cryptology–EUROCRYPT 2010, pages 62–91. Springer, 2010.

[19] Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Advances in Cryptology–CRYPTO 2012, pages 180–198. Springer, 2012.

[20] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. KSFOABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Trans. Services Computing, 10(5):715–725, 2017.

[21] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian, and Jinguang Han. Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Trans. Services Computing, 10(5):785–796, 2017.

[22] Jin Li, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, Duncan S Wong, and Dongqing Xie. Multi-authority ciphertext-policy attribute-based encryption with accountability. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, pages 386–390. ACM, 2011.

[23] Jin Li, Kui Ren, and Kwangjo Kim. A2be: Accountable attributebased encryption for abuse free access control. IACR Cryptology ePrint Archive, 2009:118, 2009.

[24] Jiaqiang Liu, Yong Li, Huandong Wang, Depeng Jin, Li Su, Lieguang Zeng, and Thanos Vasilakos. Leveraging softwaredefined networking for security policy enforcement. Inf. Sci., 327:288–299, 2016.

[25] Qiang Liu, Hao Zhang, Jiafu Wan, and Xin Chen. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. IEEE Access, 5:7001–7011, 2017.

[26] Zhen Liu, Zhenfu Cao, and Duncan S Wong. Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 475–486. ACM, 2013.

[27] Zhen Liu, Zhenfu Cao, and Duncan S Wong. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Transactions on Information Forensics and Security, 8(1):76–88, 2013.

[28] Ben Lynn et al. The pairing-based cryptography library. Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.

[29] Dalit Naor, Moni Naor, and Jeff Lotspiech. Revocation and tracing schemes for stateless receivers. In Advances in Cryptology - CRYPTO 2001, pages 41–62. Springer, 2001.

[30] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Junqing Gong, and Jie Chen. Traceable cp-abe with short ciphertexts: How to catch people selling decryption devices on ebay efficiently. In Computer Security-ESORICS 2016, pages 551–569. Springer, 2016.

[31] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei. Auditable -time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018.

[32] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei. Traceable and revocable CP-ABE with shorter ciphertexts. SCIENCE CHINA Information Sciences, 59(11):119102:1–119102:3, 2016.

[33] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei. White-box traceable cp-abe for cloud storage service: How to catch people.