International Journal of Science Engineering and Advance Technology

An Efficient and Secure Data Access Control For Cloud Storage

[1]R.Satya veni, [2]B., Mahalakshmi Rao (M.Tech CS)
[1,2]Dept. of SE, Kakinada Institute Of Engineering And Technology, Yanam road, Korangi-533461,E.G.Dist.(A.P)

ABSTRACT:

We present an official basis model of the proposed method, intended for applied cloud storage system disposition. We discourse faintness in the checking process of the session variety. Exactly, a spiteful user may modification his secret key in the meeting form, and the checking technique will flop in this case. As an extenuation, we review the key generation algorithm and improve an inspection list to perceive if the key is changed. Looking for to allay access recommendation misappropriation, we recommend CryptCloud+, are feasible consultant and revocable CPABE based cloud storage system with white-box traceability and auditing. To the top of our acquaintance, this is the originally everyday answer to protected fine-grained access control over encrypted data in cloud.

KEYWORDS: Cloud, Ciphertext, Revocation.

INTRODUCTION:

Secure cloud storage, which is an evolving cloud service, is considered to shield the privacy of outsourced data but also to deliver stretchy data access for cloud users whose data is out of corporal control. Cipher text-Policy Attribute-Based Encryption(CP-ABE) is observed as one of the greatest talented methods that may be leveraged to protected the assurance of the facility. Though, the usage of CP-ABE may harvest an unavoidable haven crack which is recognized as the mistreatment of access credential due to the inherent "all-or-nothing" decryption feature of CP-ABE. In this paper, we examine the two chief cases of access credential misuse. One is on the semi-trusted expert side, and the other is on the side of cloud user. We primarily extant a CP-ABE based cloud storage outline. By this framework, we advise two answerable expert and revocable CP-ABE systems that are completely locked in the standard model, mentioned to as ATER-CP-ABE and ATIR-CPABE, correspondingly[1-7].

LITERATURE SURVEY:

1] Zhangjie Fu, Fengxiao Huang We describe and crack the difficulties of semantic search based on conceptual graphs (CGs) over encoded subcontracted data in clouding computing (SSCG). To achieve measurable control of CGs, we enterprise a novel process that can map CGs to vectors. Succeeding, we exuberant the reimbursed results based on "text summarization score". Additionally, we recommend a basic idea for SSCG and give a suggestively amended outline to mollify the safety agreement of searchable symmetric encryption (SSE).

2] Jiguo Li, Xiaonan Lin Attribute-based encryption as the quantity of encrypted files stowed in cloud is becoming actual gigantic, which will deter effectual query processing. To transaction with above problematic, we contemporary a new cryptographic original called attribute-based encryption scheme with subcontracting key-issuing and outsourcing decryption, which can instrument keyword search function (KSF-OABE). The anticipated KSF-OABE scheme is showed locked in contradiction of chosen-plaintext attack (CPA). CSP makes part decryption task deputized by data user deprived of expressive whatever about the plaintext. Besides, the CSP can complete encrypted keyword pursuit without eloquent anything about the keywords surrounded in hatch[8-12].

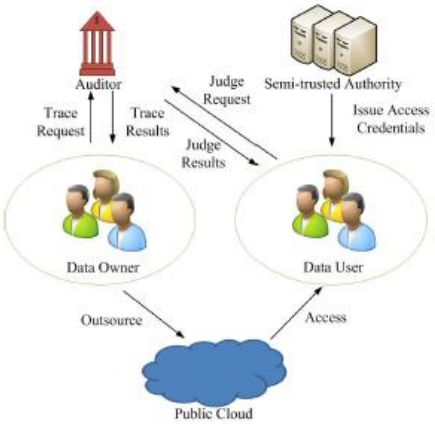
PROBLEM DEFINITION:

The trickle of any subtle student material stored in cloud could consequence in a variety of significances for the group and entities(e.g., litigation, loss of competitive advantage, and criminal charges). The CP-ABE may assistance us stop safety break from outdoor attackers. But when an insider of the group is supposed to obligate the "crimes" connected to the redeployment of decryption rights and the movement of student info in plain format for illegal monetary advances, a cloud user's access credential decryption key is frequently distributed by a semi-trusted specialist based on the characteristics the user owns.

PROPOSED APPROACH:

To alleviate the misappropriation, we suggest the initially responsible consultant and revocable CP-ABE founded cloud storage system with white-box traceability and checking, mentioned to as CryptCloud+. We also extant the haven examination and additional prove the usefulness of our system through tests. Based on the innovative ATER-CP-ABE and ATIR-CPABE, we current CryptCloud+ which is an actual and applied solution for protected cloud storage.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

Data owner:

A person who encodes its documents below a random admission regulator policy and subcontracts them to the cloud? She/he considers the time of converting in producing the cipher texts. We would highpoint that the data owner also translates his/her documents beneath his/her uninformed access rheostat policy. Nevertheless, in this paper we quintessence on the encryption of the removed keywords from documents.

Data user:

Is an individual who is appearing for credentials which hold a planned keyword, and are encrypted in a resolute time hiatus? The time interval is randomly chosen by the data user.

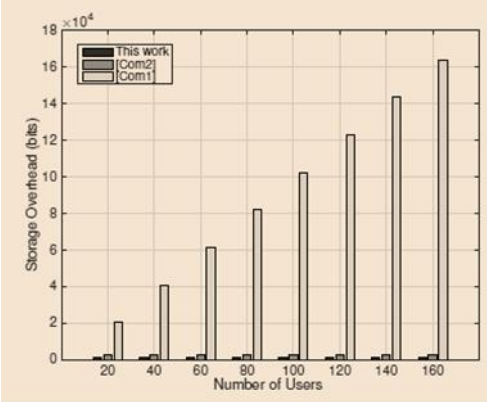
Cloud Server:

This is a unit with influential totaling and storage resources. CS stores a enormous quantity of encrypted data, and obtain the explore tokens to come across for the mandatory documents on behalf of the data user. The cloud locates the appropriate documents, and flings them back to the data user[15].

Trusted Third Party (TTP):

It is a entirely conviction individual who obtain each user's access tree, and creates their secret keys equivalent to his/her attributes set obtainable in his/her access tree. Next, the TTP propel back the users' credentials during a protected and genuine channel[13-14].

RESULTS:



Shows the system storage overhead for traitor tracing of proposed CP-ABE systems

EXTENSION WORK:

Develop attribute-driven role-based access control models such that the user role and role-permission assignments be separately constructed using policies applied on the attributes of users, roles, the objects and the environment; and the attribute-based user-role and role-permission assignment rules be applied in real-time to enforce access control decisions.

CONCLUSION:

CryptCloud+ permits us to outline and cancel malevolent cloud user's seep out permit. Our advance can be also used in the crate where the users' permits are reallocated by the semi-trusted influence. We make a note of that we may require black-box traceability, which is a stronger concept evaluate to white-box trace ability in CryptCloud. We have deal with confront of diploma leakage in CP-ABE based cloud storage system by conniving an answerable authority and revocable CryptCloud which supports white-box traceability and auditing.

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.

Miss R. SATYAVENI a student of KAKINADA INSTITUTE OF ENGINEERING ANDTECHNOLOGY,KORANGI Presently she is pursuing M.Tech [Software Engineering] from this college and she received B.Tech from ADITYA ENGINEERING COLLEGE, affiliated to JNT University, Kakinada in the year2016. Her area of interest includes Cloud Computing and in Software engineering.

Mr. B. MAHALAKSHMI RAO, well known Author and excellent teacher, Received M.Tech (CS) from a reputed university. And he is working as Associate Professor, M.Tech Computer science engineering, Kakinada institute of Engineering and Technology; He is an active member and having best teaching experience.