A NEW DELEGATION-AWARE ENCRYPTION STRATEGY TO UPDATE POLICY DATA

[1]M. Devakumar, [2]J.Bala Ambedkar

[1,2]Dept. of CSE, Kakinada Institute of Engineering & Technology, Yanam Road,, Matlapalem,Talarevu Mandal, Corangi, Andhra Pradesh 533461, India

ABSTRACT:

Empowering cryptographically enforced access controls for data facilitated in un trusted cloud is attractive for some users and associations. Be that as it may, planning proficient cryptographically enforced dynamic access control system in the cloud is as yet testing. In this work, we propose Crypt-DAC, a framework that gives reasonable cryptographic authorization of dynamic access control. A file is encoded by a symmetric key list which records a file key and a sequence of revocation keys. Accordingly, Crypt-DAC implements dynamic access control that gives proficiency, as it doesn't need expensive decryption/re encryption and uploading/re-uploading of large data at the administrator side, and security, as it promptly renounces access permissions. We use formalization structure and framework implementation to demonstrate the security and productivity of our development.

KEYWORDS: privacy, cryptographic, cloud

1] INTRODUCTION:

With the extensive progressions in cloud computing, users and associations re discovering it progressively engaging store and offer data through cloud services. Cloud service providers, (for example, Amazon, Microsoft, Apple, and so forth) give abundant cloud based services, going from small-scale personal services to large-scale industrial services. Ongoing data breaches, for example, arrivals of private photographs, have raised concerns with respect to the security of cloud-managed data. A cloud service provider is typically not secure because of plan downsides of software and framework vulnerability. All things considered, a basic issue is the way to authorize data access control on the conceivably un trusted cloud.

2] LITERATURE SURVEY:

2.1] T. Jiang ***et al***

Few explores think about the issue of secure and productive public data integrity auditing for shared dynamic data. These plans are as yet not secure against the arrangement of cloud storage server and denied bunch users during user disavowal in commonsense cloud storage framework. We sort out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector responsibility and verifier-local revocation group signature. We plan a solid plan dependent on the scheme definition. Our plan underpins people in general checking and effective user renouncement and furthermore some decent properties, for example, certainly, proficiency, countability and traceability of secure group user repudiation.

2.2] D. Nali ***et al***

We recommend a plan to cryptographically support role based access control (RBAC) in enormous associations where client roles change oftentimes. To accomplish this, we propose a safe strategy to oversee role keys and we broaden a new matching based interceded identity-based cryptographic plan to permit the implementation of ownership of numerous functions to access certain documents. We plan architecture and a set of algorithms which cryptographically authorize RBAC and take into consideration job expansion, repudiation, and delegation.

3] PROBLEM DEFINTION:

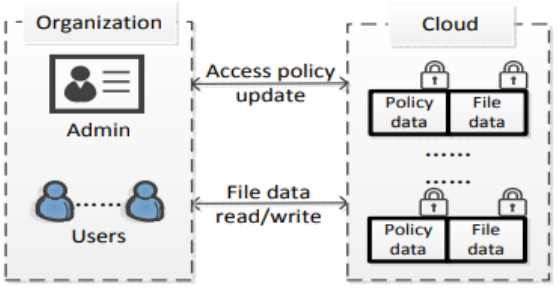
Gudes et al. [27] investigate cryptography to uphold hierarchy access control without considering dynamic policy scenarios. Akl et al. [28] propose a key task plan to simplify key management in hierarchical access control policy. Additionally, this work doesn't consider spolicy update issues. Afterward, Atallah et al. [29] propose a strategy that permits policy updates, however on account of revocation, all descendants of the influenced node in the access hierarchy of command should be updated, which includes high calculation and communication overhead.

4] PROPOSED APPROACH:

The proposed framework presents Crypt-DAC, a cryptographically upheld dynamic access control framework on un trusted cloud. Crypt DAC delegates the cloud to update encoded records in authorization revocations. In Crypt-DAC, a file is encrypted by a symmetric key list which records a file key and a sequence of

revocation keys. In a revocation, the administrator uploads another revocation key to the cloud, which encrypts the file with another layer of encryption and updates the encoded key list accordingly.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

Cloud Server

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. The end user request will be processes based on the queue.

End User

The Cloud User who has a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. The end user sends the request for corresponding file request and it will be processed in the cloud based on the queue and response to the end user.

Data Owner

The data owner uploads their data with its chunks in the cloud server. For the security purpose the data owner encrypts the data file's chunks and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

7] ALGORITHM:

Adjustable onion encryption and delayed de-onion encryption strategy:

Step 1: adjustable onion encryption strategy enable the administrator to define a tolerable bound for the file.

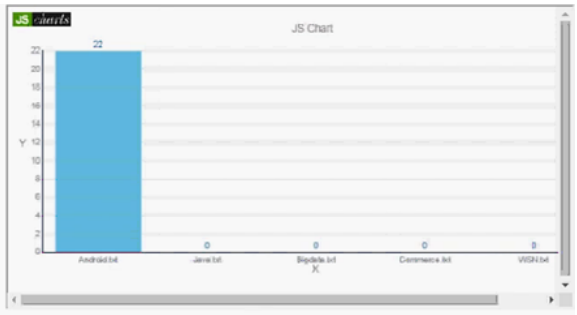
Step 2: Once the size of encryption layers reaches the bound, it can be made to not increase anymore by delegating encryption operations to the cloud.

Step 3: As a result, the administrator can flexibly adjust a tolerable bound for each file (according to file type, access pattern, etc.) to achieve a balance between efficiency and security.

Step 4: delayed de-onion encryption strategy to periodically refresh the

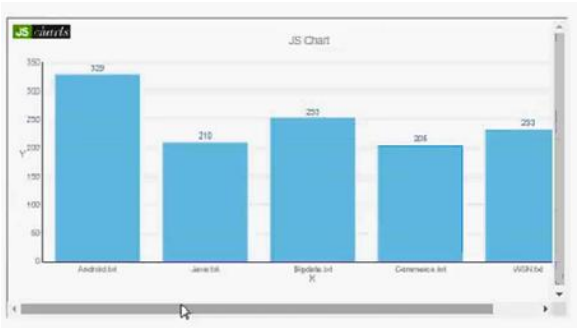
symmetric key list of the file and remove the bounded encryption layers over it through writing operations

8] RESULTS:



File rank details

The above graph shows that rank result for documents. X-axis is name of the document and Y-axis is rank.



Time delay

The above graph shows that time delay result. X-axis is name of the document and Y-axis is time.

Throughput Details

The above graph shows that Throughput result for documents. X-axis is name of the document and Y-axis is balanced flow.

9] CONCLUSION:

A framework that gives useful cryptographic implementation of dynamic access control in the possibly un trusted cloud provider.

We propose to designate the cloud to update the policy data in a privacy-preserving manner utilizing a delegation-aware encryption strategy. We propose to avoid the costly re-encryptions of file data at the administrator side utilizing a flexible onion encryption methodology.

10] EXTENSION WORK:

We introduce a cloud storage system that offers cryptographically enforced security. In contrast to other cryptographically protected cloud storage systems, our system supports a fine-grained access control mechanism and allows flexible revocations of invalid users without moving the data

and relying on the cloud service providers. Our system employs an attribute-based encryption technique to support a complex access structure that allows a user to define human readable access policies to the data in the cloud storage. In addition, our system supports a flexible revocation scheme that can revoke invalid users directly by updating the revoked users' list or indirectly by updating an epoch counter. The system administrator can choose one of these options flexibly depending on the needs. Our system also allows authorized users to update the encrypted data, and any users accessing such updated data in future can verify whether the data are modified by authorized users

11] REFERENCES:

[1] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption, in IEEE S&P, 2007.

[2] X. Wang, Y. Qi, and Z. Wang, Design and Implementation of SecPod: A Framework for Virtualization-based Security Systems, IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, 2019.

[3] J. Ren, Y. Qi, Y. Dai, X. Wang, and Y. Shi, AppSec: A Safe Execution Environment for Security Sensitive Applications, in ACM VEE, 2015.

[4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, Bounded ciphertext policy attribute based encryption, in ICALP, 2008.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in ACM CCS, 2006.

[6] J. Katz, A. Sahai, and B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, in EUROCRYPT, 2008.

[7] S. Muller and S. Katzenbeisser, Hiding the policy in cryptographic access control, in STM, 2011.

[8] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in ACM CCS, 2007.

[9] A. Sahai, and B. Waters, Fuzzy identity-based encryption, in EUROCRYPT, 2005.

[10] T. Ring, Cloud computing hit by celebgate, http://www.scmagazineuk. com/cloud-computing-hit-by-celebgate/article/370815/, 2015.

[11] X. Jin, R. Krishnan, and R. S. Sandhu, A unified attribute-based access control model covering DAC, MAC and RBAC, in DDBSec, 2012. [12] W. C. Garrison III, A.

Shull, S. Myers, and, A. J. Lee, On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud, in IEEE S&P, 2016.

[13] R. S. Sandhu, Rationale for the RBAC96 family of access control models, in ACM Workshop on RBAC, 1995.

[14] T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, Secure and Efficient Cloud Data Deduplication With Randomized Tag, IEEE Trasactions on Data Forensics and Security, vol. 12, no. 3, 2017.

[15] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, Plutus: Scalable Secure File Sharing on Untrusted Storage, in USENIX FAST, 2003

Mr. M. Devakumar is a student of Kakinada institute of Engineering & Technology, Matlapalem. Presently he is pursuing his M.Tech [Computer Science and Engineering] from this college and he received his B.Tech from Kakinada institute of Engineering & Technology, affiliated to JNT University, Kakinada in the year 2016. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. J Bala Ambedkar is working as assistant professor in Kakinada institute of Engineering & Technology, Matlapalem. He has 7 years of teaching experience. To his credit couple of publications both national and international conferences /journals.