INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 5 ISSUE 2 (2019) PAGES 4222 - 4228
RECEIVED : 16.02.2019 PUBLISHED : 19.03.2019

March 19,2019

# MONA : SECURE MULTI OWNER DATA SHARING FOR DYNAMIC GROUPS IN CLOUD

[1]Jayapradha.P, [2]Kanishka.G , [3]Maha Lakshmi.G ,[4]Monisha.L , [5]Shankar Ganesh.K

[1,2,3,4]UG Scholar,Department of Computer Science Engineering, Kingston Engineering College, Katpadi, Vellore, Tamil Nadu.

[5]Assistant Professor, Department of Computer Science Engineering, Kingston Engineering College, Katpadi, Vellore, Tamil Nadu.

## ABSTRACT

The genuine purposes of this strategy a safe multi-proprietor data sharing arrangement. It derives that any customer in the social affair can securely give data to others by the untrusted cloud. This arrangement can support dynamic social occasions. *Customer revocation can be successfully* proficient through a novel foreswearing list without updating the puzzle Keys of whatever remains of the customers. The size and count overhead of encryption are steady and Independent with the amount of revoked customers. We present a safe and security ensuring access control to customers, which guarantee any part in a social event to anonymously utilize the cloud resource. Likewise, the veritable identities of data proprietors can be revealed by the get-together executive when open deliberation happen. We give careful security examination, and perform expansive generations to show the adequacy of our arrangement to the extent limit and estimation overhead. Disseminated figuring gives a traditionalist and gainful response for sharing social event resource among cloud customers. Shockingly, sharing data in a multi-proprietor way while shielding data and identity security from an untrusted cloud is still a testing issue, in light of the constant change of the enlistment.

Keywords: cloud customers, social occasions, social event resource.

## 1. INTRODUCTION

The primary intention of our task is to sharing the information in cloud. In this paper, we exhibit that how to securely, effectively and flexibly share information with others in cloud storage. For that we propose an idea with Key- Aggregate Cryptosystem that generates cipher-text of original size such that decryption rights can be assigned on them. By combining a set of secret key, we can make a compact single key. By the use of this compact key, we can send others or can be store in a very limited secure storage. First, proprietor of the statistics Setup the public system subsequent KeyGen algorithm generates a public or master/secret key. By using this key, [1]person can convert plain text to cipher text. Next user will give input as master secret key by using Extract function; it will produce output as aggregate decryption key. This generated key is safely despatched to the receiver. Then the person with aggregaate key can decrypt the cipher text through the use of Decrypt function.We furnish formal protection analysis of our schemes in the preferred model. We also describe different utility of our schemes. In particular, our schemes provide the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.Cloud storage is gaining popularity recently. In enterprisesettings, we see the upward thrust in demand for dataoutsourcing, which assists in the strategic management ofcorporate data. It is also used as a core technology behind.

## 2.EXISTING SYSTEM

The existing device of cloud storage bloggers can let their friends view a subset of their personal images or data; an organization may grant her personnel access to a element of sensitive data. The difficult trouble is how to effectively share encrypted data. Of direction [2]users can download the encrypted records from the storage, decrypt them, then send them to others for sharing, however it loses the value of cloud storage. Users need to be able to delegate the accessrights of the sharing information to others so that they can access these information from the server directly. However, finding an efficient and impervious way to share partial data in cloud storage is no longer trivial. The receiver decrypting the authentic Message the usage of symmetric key algorithm.

## 3.LIMITATION

Increases the charges of storing and transmitting ciphertexts.

Secret keys are generally stored in the tamper-proof memory, which is fairly expensive.

The expenses and complexities involved commonly increase with the wide variety of the decryption keys to be shared.

## 4. PROPOSED SYSTEM:

In this paper, we make a decryption key as extra effective in the feel that it allows decryption of more than one ciphertexts, without increasing its size. We are introducing a public-key encryption which we name key-aggregate cryptosystem (KAC) they using AES algorithm. In KAC, users encrypt a message not only beneath a public-key, but also beneath an[3] identifier of ciphertext referred to as class. That skill the ciphertexts are similarly classified into special classes. The key proprietor holds a master-secret known as master-secret key, which can be used to extract secret keys for distinctive classes. More importantly, the extracted key have can be an mixture key which is as compact as a secret key for a single class, however aggregates the strength of many such keys, i.e., the decryption energy for any subset of ciphertext classes. The sizes of ciphertext, public-key, and master-secret key and aggregate key in our KAC schemes are all of regular size. The public device parameter has measurement linear in the quantity of ciphertext classes, however solely a small section of it is needed every time and it can be fetching on demand from large  cloud storage. Previous consequences can also obtain a comparable property offering a constant-size decryption key, however the lessons need to conform to some pre-defined hierarchical relationship. Our work is flexible in the experience that this constraint is eliminated, that is, no exceptional relation is required between the classes.

## 5. ADVANTAGES

The delegation of decryption can be efficiently carried out with the aggregate key, which is solely of constant size.

Number of ciphertext training is large.

It is convenient to key administration for encryption and decryption

## 6. LITERATURE SURVEY

1 ) Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing
Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou_Dept. of ECE, Worcester Polytechnic Institute.
This paper addresses this difficult open issue by, on one hand, defining and imposing get entry to policies primarily based on information attributes, and on the different hand, allowing the data-owner to delegate most of the computation duties concerned in fine-grained facts get admission to control to untrusted cloud servers besides disclosing the underlying facts contents. We reap this purpose by using exploiting and uniquely combining methods of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme additionally has salient properties of user get admission to privilege confide/ntiality and consumer secret key accountability

2)Plutus: Scalable impervious file sharing on untrusted storage

MaheshSan Francisco, CA, USA

March 31–April 2, 2003

This paper has introduced novel uses of cryptographic primitives utilized to the problem of impervious storage in the presence of privacy less servers and a desire for owner managed key distribution. Eliminating nearly all necessities for server have confidence (we still require servers no longer to wreck information two although we can notice if they do) and keeping key distribution (and consequently get entry to control) in the hands of man or woman information proprietors gives a foundation for a invulnerable storage device that can protect and share data at very giant scales and across have confidence boundaries.

3) SiRiUS: Securing Remote Untrusted Storage

Eu-Jin Goh, HovavShacham, NagendraModadugu, Dan BonehStanford University

This paper provides SiRiUS, a invulnerable file machine designed to be layered over insecure network and P2P file structures such as NFS, CIFS, OceanStore, and Yahoo! Briefcase. SiRiUS assumes the community storage is untrusted and affords its very own read-write cryptographic access manipulate for file stage sharing. Key management and revocation is easy with minimal out-of-band communication. File machine freshness ensures are supported through SiRiUS the usage of hash tree constructions.

SiRiUS consists of a novel approach of performing file random get entry to in a cryptographic file system barring the use of a block server.

4) Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing

Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen

In this paper proposed scheme is characterized by way of providing the facts confidentiality on touchy archives stored in cloud, nameless authentication on person access,and provenance tracking on disputed documents. With the provable protection techniques, we formally demonstrate the proposed scheme is impenetrable in the popular model.

5) Ciphertext-Policy Attribute-Based Encryption :An Expressive, E-client, and Provably Secure Realization

Brent Waters _University of Texas at Austin

This Paper present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) beneath concrete and non-interactive cryptographic assumptions in the general model. Our options permit any encryptor to specify get admission to manipulate in terms of any access formulation over the attributes in the system. In our most e_client system, ciphertext size, encryption, and decryption time scales linearly with the complexity of the get entry to formula. The only preceding work to attain these parameters was once constrained to a proof in the normal crew model.

6) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

Vipul GoyalOmkant PandeyyAmitSahaizBrent Waters

This Paper provides extra touchy records is shared and saved by means of third-party websites on the internet services, there will be a need to transform the encrypt data stored at these sites. One downside of encrypting statistics is that it can be selectively [5-6]shared only at a coarse-grained level (i.e., giving an other celebration your non-public key). We advance a new cryptosystem for ¯ne-grained sharing ofen crypted information that we name Key-Policy Attribute-Based Encryption (KP-ABE).We reveal the applicability of our building to sharing of audit-log records and broadcast encryption.

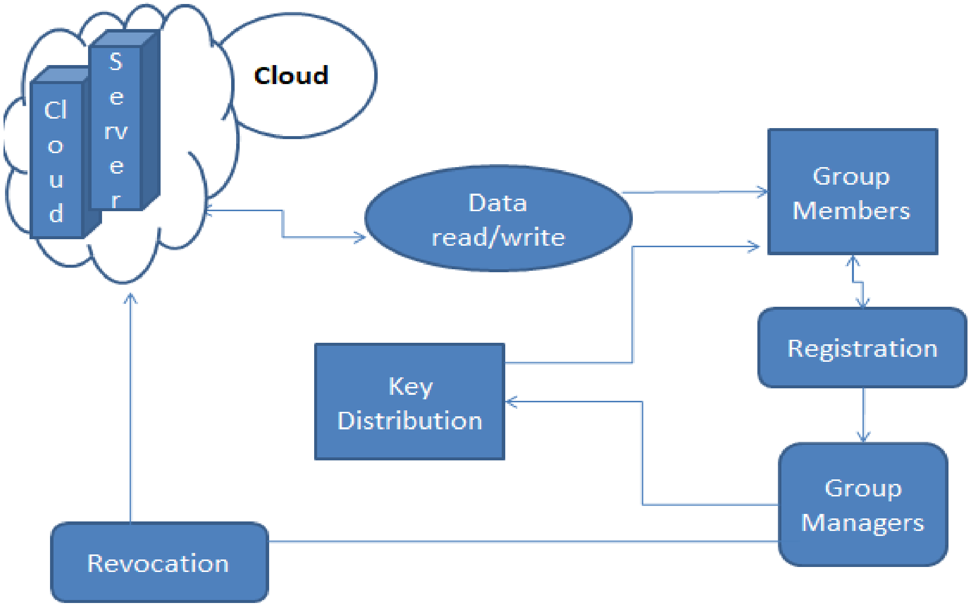
7) Revocation and Tracing Schemes for Stateless Receivers

Dalit Naor1, Moni Naor, and Je Lotspiech

This paper grant a usual traitor tracing mechanism that can be built-in with any Subset-Cover revocation scheme that satises a bifurcation property". This mechanism does no longer want an a priori certain on the number of traitors and does no longer increase the message size through a great deal in contrast to the revocation of the equal set of traitors.

## 7.SYSTEM ARCHITECTURE

.



For the registration of user with identity ID the team supervisor randomly selects a number. Then the crew manager adds into the team consumer listing which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature era and file decryption.

User revocation is carried out by means of the group supervisor via a public available. Revocation list primarily based on which group individuals can encrypt their facts documents and make sure the confidentiality in opposition to the revoked users. By using facts sharing offerings in cloud user can able alter statistics as a crew on cloud. Integrity of these offerings can be increased the usage of signature of public existing users on group. Shared records is divided into blocks.

To store and share a statistics file in the cloud, a team member performs to getting the revocation list from the cloud. In this step, the member sends the crew identity ID team as a request to the cloud. Verifying the validity of the revocation list. File stored in the cloud can be deleted with the aid of either the team supervisor or the facts owner.

To get right of entry to the cloud, a person wants to compute a team signature for his/her authentication. The employed group signature scheme can be considered as a variant of the brief crew signature which inherits the inherent enforceability property, nameless authentication, and monitoring functionality.

## 8.CONCLUSION

In this paper, we sketch Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage. In Mona, a consumer is able to share information with others in the team without revealing identity privateness to the cloud. Additionally, Mona helps efficient consumer revocation and new consumer joining. More specially, environment friendly person revocation can be executed through a public revocation list except updating the personal keys of the last users, and new customers can immediately decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation price are constant. Extensive analyses exhibit that our proposed scheme satisfies the preferred protection necessities and ensures effectivity as well. proposed a cryptographic storage gadget that permits impervious file sharing on untrusted servers, named Plutus. By dividing archives into file businesses and encrypting every file group with a special file-block key, the facts proprietor can share the file organizations with others via turning in the corresponding lockbox key, the place the lock box key is used to encrypt the block keys. However, it brings about a large key distribution overhead for large-scale file sharing. Additionally, the file-block key wishes to be updated and disbursed once more for a person revocation.

## FUTURE WORK

Finally, as the subsequent step in our research, we purpose to raise out greater experiments the use of greater information and also from special academic ranges (primary, secondary, and higher) to take a look at whether or not the equal overall performance consequences are bought with unique DM approaches. As future work, we can mention the following:

1) To improve our own algorithm for classification/prediction based totally on grammar the usage of genetic programming that can be compared versus traditional algorithms.

2) To predict the scholar failure as quickly as possible. The formerly the better, in order to realize college students at chance in time before it is too late.

3) To propose actions for supporting college students recognized inside the threat group. Then, to take a look at the rate of the instances it is possible to avert the fail or dropout of that scholar until now detected.

## REFERENCES

1.K. Kent and M. Souppaya. (1992). Guide to Computer Security Log Management, NIST Special Publication 800-92 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

2. U.S. Department of Health and Human Services. (2011, Sep.). HIPAA—General Information [Online]. Available: https://www.cms.gov/hipaageninfo

3 PCI Security Standards Council. (2006, Sep.) Payment Card Industry (PCI) Data Security Standard—Security Audit Procedures Version 1.1[Online].Available: https://www.pcisecuritystandards.org/pdfs/pci−audit−procedures−v1-1.pdf

4. Sarbanes-Oxley Act 2002. (2002, Sep.). A Guide to the Sarbanes-Oxley Act [Online]. Available: http://www.soxlaw.com/

5. C. Lonvick, The BSD Syslog Protocol, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.

6.D. New and M. Rose, Reliable Delivery for Syslog, Request for Comment RFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.