ISSN 2320 – 2602
Volume 4 No.5, May 2015
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/ijacst/static/pdf/file/ijacst01452015.pdf

# DECENTRALIZED APPROACH FOR CONTROLLING RECOGNIZED FILE SHARING SYSTEM IN CLOUD

**Ali HasanKamil Alsaadawi[1],Y V K Sudhakar[2]**
[1]M.Sc (Computer Science) Mahatma Gandhi College Affiliated to AcharyaNagarjuna University Guntur, AP, India.
ali.gharaf88@gmail.com
[2]M.Tech (CSE) Mahatma Gandhi College Affiliated to AcharyaNagarjuna University Guntur, AP,
India,sudakartechcs@yahoo.com

## ABSTRACT

Security and privacy area unit important problems in cloud computing, we tend to propose a brand new information sharing has ne'er been easier with the advances of cloud computing, associated associate correct analysis on the shared information provides an array of advantages to each the society and people. Information sharing with an outsized range of participants should take under consideration many problems, as well as potency, information integrity and privacy of knowledge owner. Ring signature could be a promising candidate to construct associate anonymous and authentic information sharing system. It permits an information knowledge owner to anonymously certify his data which may be place into the cloud for storage or analysis purpose. Nevertheless the expensive certificate verification within the ancient public key infrastructure (PKI) Setting becomes a bottleneck for this answer to be ascendible. Identity-based (ID-based) ring signature, that eliminates the method of certificate verification, are often used instead. There area unit 3 users: creator, reader & author. Creator receives a token from a trustee i.e. organization when giving ID to the trustee. There was multiple of Key Distribution Centers (KDC) which may be scattered. A creator provides their token to at least one or a lot of KDC's then creator receives keys for secret writing & coding and for linguistic communication from KDC's. The message is encrypted below access policy which suggests it decides United Nations agency will access the information hold on within the cloud. Creator decides on a claim policy to prove her credibleness and signs the message below this claim. The cipher text is distributed to the cloud. The cloud verifies the signature and stores the cipher text. Once a browser desires to read, the cloud sends cipher text. If the user has attributes matching with access policy, it will decipher and obtain back original message.

**KEY WORDS:** Cloud Computing,KDC (Key Distribution Centers), Public key infrastructure (PKI), Authentication**.**

## 1.INTRODUCTION

Cloud Computing has been unreal because the next-generation design of IT enterprise, attributable to its long list of new benefits within the IT history: on-demand self-service, present network access, location freelance resource pooling, speedy resource snap, usage-based evaluation and transference of risk. As a riotous technology with profound implications, Cloud Computing is remodeling the terribly nature of however businesses use data technology. One basic facet of this paradigm shifting is that information is being centralized or outsourced into the Cloud. From users' perspective, together with each people and enterprises, storing information remotely into the cloud in an exceedingly versatile on-demand manner brings appealing benefits: relief of the burden for storage management, universal information access with freelance geographical locations, and shunning of cost on hardware, software, and personnel maintenances, etc . whereas these benefits of exploitation clouds ar incontestable , attributable to the opaqueness of the Cloud—as separate body entities, the interior operation details of cloud service suppliers (CSP) might not be well-known by cloud users—data outsourcing is additionally relinquishing user's final management over the fate of their information. As a result, the correctness of the info within the cloud is being place in danger attributable to the subsequent reasons. initial of all, though the infrastructures underneath the cloud ar way more powerful and reliable than personal computing devices, they're still facing the broad vary of each internal and external threats for information integrity. samples of outages and security breaches of noteworthy cloud services seem from time to time . Secondly, for the advantages of their own, there do exist numerous motivations for cloud service suppliers to behave undependably. Towards the cloud users relating to the standing of their outsourced information. Examples embrace cloud service suppliers, for financial reasons, reclaiming storage by discarding information that has not been or isn't accessed, or perhaps concealing information loss incidents therefore on maintain a name . In short, though outsourcing information into the cloud is economically enticing for the value and complexness of semipermanent large-scale information storage, it doesn't provide any guarantee on information integrity and accessibility. This downside, if not properly self-addressed, could impede the eminent readying of the cloud design.

## 2.RELATED WORK

S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” [1]
In this paper, we tend to propose a brand new privacy conserving attested access management theme for securing information in clouds. Within the projected theme, the cloud verifies the credibleness of the user while not knowing the user’s identity before storing info. Our theme additionally has the another feature of access management during which solely valid users are able to decipher the hold on info. The theme prevents replay attacks and supports creation, modification, and reading information hold on within the cloud. Moreover, our authentication and access management theme is localized and sturdy, not like alternative access management schemes designed for clouds that are centralized. The communication, computation, and storage overheads ar like centralized approaches.
J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” [3]
With recent important development within the transportable device market, cloud computing is obtaining additional and additional used. several sensitive knowledge ar hold on in cloud central servers. to confirm privacy, these knowledge ar typically encrypted before being uploaded—making file looking sophisticated. though previous cloud computing searchable secret writing schemes permit users to look encrypted knowledge by keywords firmly, these techniques solely support precise keyword search and can fail if there ar some orthography errors or if some morphological variants of words ar used. during this paper, we offer the answer for fuzzy keyword search over encrypted cloud knowledge. K-grams is employed to supply fuzzy results. For security reasons, we tend to use 2 separate servers that can't communicate with one another. Our experiment result shows that our system is effective and ascendable to handle sizable amount of encrypted files.
S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” [9]
Ciphertext-Policy Attribute primarily based cryptography (CP-ABE) may be a promising scientific discipline primitive for fine-grained access management of shared knowledge. In CP-ABE, every user is related to a collection of attributes and knowledge ar encrypted with access structures on attributes. A user is in a position to decode a ciphertext if and on condition that his attributes satisfy the ciphertext access structure. Beside this basic property, sensible applications sometimes produce other needs. during this paper we tend to concentrate on a vital issue of attribute revocation that is cumbersome for CP-ABE schemes. especially, we tend to resolve this difficult issue by considering a lot of sensible eventualities within which semi-trustable on-line proxy servers ar out there. As compared to existing schemes, our projected answer allows the authority to revoke user attributes with nominal effort. we tend to win this by unambiguously desegregation the technique of proxy re-encryption with CP-ABE, and modify the authority to delegate most of effortful tasks to proxy servers. Formal analysis shows that our projected theme is incontrovertibly secure against chosen ciphertext attacks. additionally, we tend to show that our technique may be applicable to the Key-Policy Attribute primarily based cryptography (KP-ABE) counterpart.
R.L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” [13]
In this paper we have a tendency to formalize the notion of a hoop signature, that makes it potential to specify a group of potential signers while not revealing that member truly made the signature. in contrast to cluster signatures, ring signatures don't have any cluster managers, no setup procedures, no revocation procedures, and no coordination: any user will opt for any set of potential signers that has himself, and sign any message by exploitation his secret key and also the others’ public keys, while not obtaining their approval or help. Ring signatures give a chic thanks to leak authoritative secrets in AN anonymous manner, to sign casual email in a very manner which might solely be verified by its meant recipient, and to unravel alternative issues in multiparty computations. the most contribution of this paper may be a new construction of such signatures that is categorically signer-ambiguous, demonstrably secure within the random oracle model, and exceptionally efficient: adding every ring member will increase the price of language or verificatory by one standard multiplication and one trigonal coding.

## 3.PREVIOUS WORK

Considering information privacy, a conventional thanks to guarantee it's to have faith in the server to enforce the access management once authentication, which implies any surprising privilege step-up can expose all information. in a very shared-tenancy cloud computing atmosphere, things become even worse.

Regarding convenience of files, there area unit a series of cryptographical schemes that go as so much as permitting a third-party auditor to see the provision of files on behalf of the information owner while not leaky something regarding the information, or while not compromising the information homeowners obscurity. Likewise, cloud users most likely won't hold the belief that the cloud server is doing an honest job in terms of confidentiality.

A cryptographical resolution, with established security relied on number-theoretic assumptions is additional fascinating, whenever the user isn't absolutely pleased with trusting the safety of the VM or the honesty of the technical employees.

### 3.1 Limitations

- correctness of the info within the cloud is being place in danger
- data integrity
- The prices and complexities concerned usually increase with the amount of the decipherment keys to be shared.
- The encoding key and decipherment key ar completely different publicly key encoding.

## 4.PROPOSED WORK

In this paper, we have a tendency to study a way to build a coding key additional powerful within the sense that it permits coding of multiple cipher texts, while not increasing its size. Specifically, our drawback statement is "To style associate degree economical public-key cryptography theme that supports versatile delegation within the sense that any set of the cipher texts (produced by the cryptography scheme) is decryptable by a constant-size coding key (generated by the owner of the master-secret key)." we have a tendency to solve this drawback by introducing a special variety of public-key cryptography that we have a tendency to decision key-aggregate cryptosystem (KAC). In KAC, users cipher a message not solely underneath a public-key, however additionally underneath associate degree symbol of cipher text referred to as category. which means the cipher texts square measure additional classified into totally different categories. The key owner holds a master-secret referred to as master-secret key, which may be accustomed extract secret keys for various categories. additional significantly, the extracted key have is associate degree mixture key that is as compact as a secret key for one category, however aggregates the ability of the many such keys, i.e., the coding power for any set of cipher text categories.Figure 1 shows the architecture diagram ofthe proposed system.

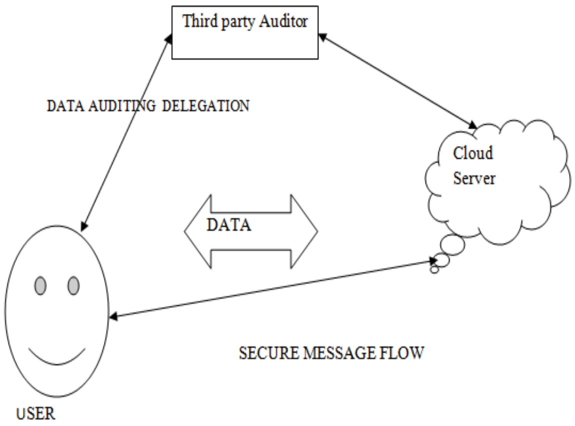

Figure.1architecture diagram ofthe proposed system.

### 4.1 Advantages

- The extracted key have may be Associate in nursing mixture key that is as compact as a secret key for one category.
- The delegation of decoding may be with efficiency enforced with the combination key.
- Storage correctness
- Privacy conserving

## 5.MODULES DESCRIPTION:

### 5.1 Secure Storage:

In this module, the user registration method is completed by the admin. Here each user's offer their personal details for registration method. once registration each user can get associate degree ID for accessing the cloud area. If any of the user needs to edit their data they need submit the main points to the admin at that time the admin can do the edit and update data method. This method is controlled by the Admin. during this module, each user's share their data and data's in their own cloud area provided by the admin. That data could also be sensitive or vital data's. For providing security for his or her data each user's storing the knowledge in their specific cloud. Registered users solely will store the information in cloud[2][4][7].

### 5.2 Key Re-Authentication:

In this module, the data and data's shared by the user within the cloud is encrypted by victimization MES (Multi secret writing Standard) algorithmic rule. All the data shared by each user is encrypted supported the info sensitivity and hold on within the cloud. Involves in consumer aspect configuration, performs 2 actions. the 2 actions square measure access management and permission management. Access management - MES algorithmic rule. Permission management –Iconic secret writing algorithmic rule. Access management method relies on the server management options. Permission management method relies on the consumer management options[5][6].

### 5.3 Integrity Checking:

Integrity checking is that the method of examination the encrypted info with altered cipher text. If there's any amendment in detection a message can send to the user that the coding method isn't done properly. If there's no amendment in detection suggests that then it'll enable doing ensuing method. Integrity checking is especially used for anti-malware controls. during this module, the encrypted knowledge is decrypted by the user victimisation the general public key of owner of the info. decipherment is that the method of changing cipher text into plain text. MES rule is employed for encrypting and decrypting the knowledge. The user will read the info and can also transfer the info with high security[10][12].

### 5.4 Data Forwarding:

In this module, the encrypted information or info keep within the cloud is forwarded to a different user account by victimization that user’s public key. If any user desires to share their info with their friends or somebody they'll directly forward the encrypted information to them. while not downloading the info the user will forward the data to a different user. Secure information Forwarding is enforced by police investigation flag generation wherever for sharing flags are 0-1 and wherever for forwarding flags 1-1 is detected. Is flag 1-1 is detected then by applying Filtering technique data’s are filtered out[8][11].

## 6.CONCLUSION

We have introduced a decentralized access system with anonymous authentication, which provides consumer resignation additionally prevents replay attacks. The cloud doesn't understand the identity of the consumer UN agency saves knowledge, but simply checks the client's certifications. Key dissemination is disbursed in an exceedingly decentralized manner.

## REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc. IEEE/ACM Int’l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[6] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-Based Cloud Computing,” Proc. Third Int’l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[8] D.F. Ferraiolo and D.R. Kuhn, “Role-Based Access Controls,” Proc. 15th Nat’l Computer Security Conf., 1992.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.

[10] G. Wang, Q. Liu, and J. Wu, “Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,” Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[11] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,” Proc. IEEE 10th Int’l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[12] S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.

[13] R.L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” Proc. Seventh Int’l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.