International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Deniable Encryption for Audit Free Cloud Storage

M.Rajya Lakshmi
M.Tech, Computer Science
Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.
V.Ramesh
Assistant Professor , Department of CSE
Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.
Dr. I.Satyanarayana
PRINCIPAL
Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.

ABSTRACT: Cloud storage offerings have emerge as increasinglywellknown. On the grounds that of the value of privateness, many cloudstorage encryption schemes had been proposed to protectiondata from the people that shouldn't have access. There are extraordinary varieties ofABE schemes and this article highlights the aspects of multiauthority attribute based encryption (MA-ABE) schemes. A multiauthority ABE method consists of any quantity attribute authoritiesand any number of users. A suite of global public parameters isoutlined in the system. A user can select an attribute authority andreceive the corresponding decryption keys. The authority executesthe corresponding attribute key iteration algorithm and the effectis returned to the user.

KEYWORDS-Deniable encryption, Attribute Based Encryption andMulti Authority-Attribute Based Encryption

I. INTRODUCTION

Cloud storage is a form of data storage where the digital data isstored in logical pools, the physical storage span multiple servers(and often locations), and the physical environment is typicallyowned and handled by a hosting organization. These cloudstorage providers are answerable for keeping the data availableand accessible, and the physical environment protected andrunning. Different organizations buy or lease storage capacityfrom the providers to store customer application data [1]. Cloudstorage services may be accessed through a co-located cloudcomputer service, a web service application programminginterface (API)[2] or by applications that utilize the API, such ascloud desktop storage, a gateway or Web- based contentmanagement systems. In the cloud storage environmentcustomers can store their data on the cloud and access their datafrom anywhere at any time by connecting to a network [3].

Because of user privacy, the data stored on the cloud is normallyencrypted and safe guarded from access by other users [4].Considering the collaborative property of the cloud data,attribute-based encryption (ABE) is regarded as one of the mostsuitable encryption schemes for cloud storage. Attribute-basedencryption is a kind of public-key encryption in which the secretkey of a user and the ciphertext are reliant upon attributes. Insuch a structure, the decryption of a ciphertext is achievable onlyif the set of attributes of the user key equals the attributes of the ciphertext.[5].

II. RELATED WORKS

In [2] authors Mazhar Al, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, Albert Y. Zomaya [1]the general public cloud outsourced data have to be secured. Unauthorized data entry via different users and procedures (whetherunintentionally or deliberately) need to be averted. A cloud ought to ensure throughput, reliability, and security. A keycomponent making a choice on a cloud throughput that outlets data is the data retrieval time. In enormous-scale methods, the datareliability issues, data availability, and response time are dealing with with data replication approaches. Nonetheless, replicasdata over a quantity of nodes increases the intrusion surface for that right information. For occurrences, storing a filewith m duplicate in a cloud alternatively than one replica raises a node probability keeping file to be chosen as attackvictim,from 1/n to m/n , where n is the complete quantity of nodes. So as to deduce that each safety and performance for thenext new release enormous-scale techniques turns into important, such as clouds. Hence, it proposes, we collectively procedurethe difficulty of safety and performance as a data relaxed predicament. We started Division and Replication of data in theCloud for most efficient efficiency and security (DROPS) that legislatively fragments user files into pieces and replicatesthem at strategic locations inside the cloud. The file division into fragments is carried out established on a given user standardssuch that the individual fragments does no longer consist any significant data. Every cloud node contains a particularfragment to develop the protection for data. A successful attack on a single node have to not disclose the opposite fragments areas within the cloud. To toughen data retrieval time, the nodes have selected based on the centrality measures thatensure an elevated access time. Furthermore to beef up the retrieval time, we legislatively replicate fragments generatethe best read/write requests over these nodes. The nodes determination is performing in two phases. In the first section, thenodes are opting for established on the fragments preliminary placement on the centrality measures. In the second segment, the nodesare making a choice on for replication.

Alessandro Mei, Luigi V. Mancini, and Sushil Jajodia,[9] It pursuits at designing a solution based on a colossal quantityof servers correlative to the decentralized algorithms so that guarantee the availability and the system'sfunctionalities scalability. The file method services does no longer incorporate centralized server, only a collection of cooperating nodesto provide data storage, universal access, and restoration to remote customers in a scalable and dynamically reconfigurable way.Only purchasers have trusted at the same time all servers are un-trusted; this transformation strongly influence to the security and availabilitymodels. In a fragmentation scheme, a file f is division into n fragments, all f ragments have signed and disbursed to nremote servers, one fragment per server. The user can reconstruct file f by means of accessing fragments arbitrarily chosen. Thealgorithm works within the learn-m-write-all context. On the whole, m fragments read are performed from the closest serversamongst those who retailer the n file fragments. A write is carried out to all of the n servers. When m=1, a fragmentationscheme coincides with an scheme for n replication, where n copies (replicas) of file f are saved to n distinctive remoteservers. A gigantic-scale distributed file process normally bases file availability, confidentiality, and integrity on acombination of file fragmentation, file replication, and file encryption systems. This paper proposes a model todetermine file assurance stored in such a process, the place the file assurance is the likelihood for file has now not beencompromised underneath the belief that the method is the goal attack victorious.

Boyang Wang, Baochun Li, Hui Li[10] the data stored in an un-relied on cloud may just lost readily or corrupted,on account that of hardware failures and human blunders . To defend the cloud data integrity, it's high-quality to perform publicintroducing with the intention to auditing a third party auditor (TPA), who offers its auditing service with extra robustcomputation and conversation data than usual users. We recommend Oruta, a brand new privateness retaining publicauditing mechanism for shared data in an un-trusted cloud. In Oruta, we make use of ring signatures to constructhomomorphic authenticators so that the third party auditor can verify the shared data integrity for a customers group with outretrieving the whole data , at the same time on every block in shared data the signer identification kept private from the TPA. Furthermore,we further prolong our mechanism to providing batch auditing, which may audit multiple data shared simultaneously ina single auditing challenge. Meanwhile, Oruta extend to use random masking to aid data privateness in the course of public auditing,and leverage index hash tables to help totally mighty operations on shared data. An strong operation suggests aninsert, delete or update operation on a single block in shared data.

Kui Ren ,Cong Wang, Qian, , Ning Cao, Wenjing Lou, [11] propose an active and delicate dispensed storageauthentication scheme with unique dynamic data help to ensure the correctness and users' data availability in thecloud. We rely on technology assure making improvements to code in the file distribution measures to furnish redundancies and guaranteethe data perseverance towards Byzantine servers, the place a storage server may just ruin down in random methods. Thisdevelopment greatly lowers the conversation and storage overhead as in comparison with the traditional replication established file distribution approach. By way of applying the homomorphic token with authenticated erasure-coded data haveallotted, our scheme achieves the storage correctness assurance as well as data error localization. At any time datacorruption has disclosed in the course of the storage correctness authentication, our scheme can just about warranty the data errorssimultaneous localization, i.e., the misbehaving server(s) identification. With a view to strike a good stability between errorflexibility and data dynamics, we extra analyze our token computation the algebraic property and erasure-coded data,and assess the best way to conventionally support dynamic operation on data blocks, while preserving the storagecorrectness assurance on the same degree. In an effort to keep the time, computation resources, and even the associated clientson-line burden, we also furnish the proposed the extension predominant scheme is used to help third-party auditing, whereclients can cautiously delegate the integrity analyzing duties to third-party auditors (TPA) and be care-free to use the cloudstorage assistances.

III. SYSTEM AND METHODOLOGY

Most deniable public key schemes are bitwise, which meansthese schemes be competent to system one bit a time. As a result, bitwisedeniable encryption schemes are incompetent for actual use,mainly within the cloud storage service case. To resolve thischallenge, viewed a hybrid encryption scheme thatconcurrently makes use of symmetric and asymmetric encryption. Theyuse a deniably encrypted plan-forward symmetric data encryptionkey, while actual data are encrypted by using a symmetric keyencryption mechanism. Most of the time deniable encryption schemeshave decryption error problems. These errors come from theviewed decryption mechanisms. Uses the subset resolutionmechanism for decryption. The receiver decides the decryptedmessage in line with the subset choice outcome. If the senderwants an element from the common set but unfortunately thedetail is located in the designated subset, then an error happens.The equal error occurs in all obvious set-based deniableencryption schemes. Scope the coverage of a file might be unusedto under the request through the patron, when concluding the timeof the contract or completely transfer the records starting with one cloudthen onto the next cloud nature's domain. The position when anyof the above criteria exists the coverage will likely be rejecting and thesignificant director will thoroughly withdraw from the public key of theassociated file. So no user can prefer up the control key of arepudiated file in future. As a result of this reason we will say the file iswithout doubt erased. To get good the file, the user must ask for thekey controller to fabricate the public key. For that the person have got tobe tested. The important thing coverage attribute based encryption general isutilized for file entry which is verified by the use of anattribute connected with the file.

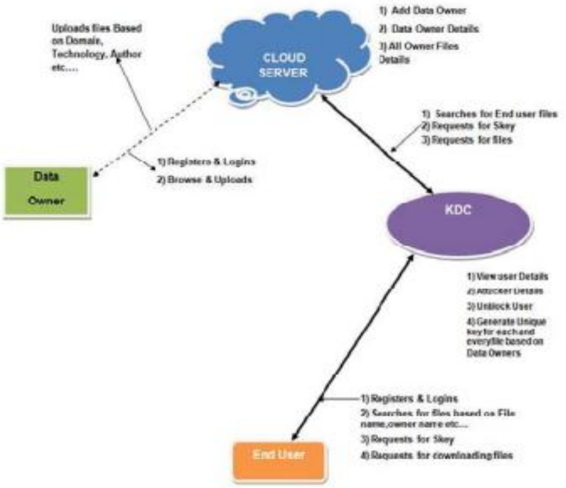
Uploads files Based on Domain, Technology, Author etc....
CLOUD SERVER
1) Add Data Owner
2) Data Owner Details
3) All Owner Files Details
1) Searches for End user files
2) Requests for Skey
3) Requests for files
1) Registers & Logins
2) Browse & Uploads
Data Owner
KDC
1) View user Details
2) Attacker Details
3) Unblock User
4) Generate Unique key for each and everyfile based on Data Owners
1) Registers & Logins
2) Searches for files based on File name,owner name etc....
3) Requests for Skey
4) Requests for downloading files
End User

Fig.1System Architecture

In this work, there is a steady environment for deniableencryption scheme. With the aid of regular atmosphere, signifies that oneencryption environment can be used for multiple encryptiontimes with out process updates. The opened receiver proof will have tolook convincing for all cipher texts beneath this atmosphere,in spite of whether or not a cipher textual content is normally encrypted ordeniably encrypted. The deniability of this scheme comes fromthe secret of the subgroup venture, which is determined simplestonce in the process setup phase. Through the canceling property andthe proper subgroup undertaking, can assemble the launched falsekey to decrypt ordinary cipher texts correctly.

A. Deniable encryption process

Deniable encryption includes senders and receivers developingplausible fake proof of false data in cipher texts such thatoutside coercers are pleased. Notice that deniability comes fromthe reality that coercers can not verify the proposed tips isflawed and as a result no motive to decline the given evidence.This method tries to overall block coercion efforts on the grounds thatcoercers understand that their efforts will probably be useless. We make use of this concept such that cloud storage providers may give audit-freestorage offerings. Within the cloud storage problem, information owners whostore their information on the cloud are identical to senders in the deniableencryption scheme. Most people who can access the encrypted dataplay the role of receiver within the deniable encryption scheme,together with the cloud storage vendors themselves, who haveprocess vast secrets and have to be able to decrypt all encrypteddata. We make use of ABE traits for securing storeddata with a first-rate-grained access manipulate mechanism and deniableencryption to avert outside auditing.

 Data Owner

In this module, the cloud server adds data owner byRegistering with their details like owner name,password, email, organization and address, The Data owner Logins by user name and password. The data owner browses and uploads their data in the cloudserver by providing details Domain (Cloud computing,Data mining, networking, sensor networking, adhocnetworking), Technology (Java, Dot net, SAP, PHP,NS2), Author name and publication. For the securitypurpose the Data owner encrypts data as well asencrypted keyword-index stores to the cloud Server.

 Cloud Server

The cloud server is responsible for data storage andfiles authorization and file search for an end user. Theencrypted data file contents will be stored with theirtags such as file name, domain, Technology, Author,Publication, secret key, digital sign, date and time andowner name. The data owner is also responsible foradding data owner and to view the data owner files.The owner can conduct keyword search operations onbehalf of the data users, the keyword search based onkeywords (Author, Technology, Domain, publishers)will be sent to the Trust authority. If all are true then itwill send to the corresponding user or he will becaptured as attacker. The cloud server can also act asattacker to modify the data which will be auditing bythe audit cloud.

 Data Integrity

Data Integrity is very important in database operationsin particular and Data warehousing and Businessintelligence in general. Because Data Integrity ensuredthat data is of high quality, correct, consistent andaccessible.

 KDC

The KDC allows clients and cloud applications tosimultaneously data user services from and route data to cloud. Module issues credentials to the data users.The credentials are sent over authenticated privatechannels. It is responsible of searching, requesting thefile to cloud server, generating secret key for each andevery files based on data owner and provides to theData user.

 Data Consumer(Data User/End User)

In this module, the user is responsible of searching thefiles in cloud server by providing attributes likeTechnology, author name, publisher, Domain(cloudcomputing, network security,). The data consumer canrequest the secret key to cloud server via KDC andthen the Data Consumer can access the data file withthe encrypted key, so if User access the file by wrongKey then the user will consider as malicious users andblocked the User.

IV. CONCLUSION

We endorse a strategy which offers with cloud storage safety and top of the line performance in phrases ofretrieval time. A deniable MA-ABE scheme is an audit-free cloud storageservice. The deniability feature makes force invalid, and theAttribute based Encryption belongings guarantee at ease clouddata sharing with a secure access control approach. Thisscheme presents a likely strategy to struggle next to dissipatedintervention with the correct of privacy.

REFERENCES

[1] Mazhar Al, Kashif Bilal, Samee U. Khan, BharadwajVeeravalli, Keqin Li, Albert Y. Zomaya

"DROPS: Division and Replication of D atainCloud for Optimal Performance and Security" DOI 10.1109/TCC.2015.2400460, IEEE Transactions on Cloud Computing

[2] Frederick R. Carlson Saint Petersburg College Saint Petersburg, Florida 352-586-2621 "Security Analysis of Cloud Computing"fcarlson@ieee.org

[3] K.L.NEELA et al. "A Survey on Security Issues and Vulnerabilities on Cloud Computing"International Journal of Computer Science &Engineering Technology (IJCSET).

[4] MukeshSinghal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-JoonAhn, Elisa Bertino," Collaboration inMulticloud Computing Environments: Framework and Security Issues IEEE Transactions on Cloud Computing VOL:46 NO:2 YEAR 2013

[5] Po-Wen Chi and Chin-Laung Lei," Audit-Free Cloud Storage via Deniable Attribute-based Encryption" DOI 10.1109/TCC.2015.2424882,IEEE Transactions on Cloud Computing

[6] D. Boneh and X. Boyen. "Efficient selective-id secure identitybasedencryption without random oracles". In EUROCRYPT, pages 223-238,2004.

[7] D. Boneh and X. Boyen. "Secure identity based encryption withoutrandomoracles". InCRYPTO, pages 443-459, 2004.

[8] D. Boneh, X. Boyen, and E. Goh. "Hierarchical identity basedrandomoracles". InCRYPTO, pages 443-459, 2004.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. "Publickeyencryption withkeyword search". In EUROCRYPT, pages 506-522, 2004.

[10] D. Boneh and M. Franklin. "Identity based encryption from theweilpairing". In CRYPTO,pages 213-229, 2001.

[11] D. Boneh, A. Sahai, and B. Waters. "Fully collusion resistant traitortracingwith shortciphertexts and private keys". In EUROCRYPT,pages 573-592, 2006.

[12] R. Bradshaw, J. Holt, and K. Seamons. "Concealing complexpolicies withhidden Credentials". In ACM Conference onComputer and CommunicationsSecurity, pages146-157,2004.

[13] J. Camenisch and A. Lysyanskaya. "An efficient system fornontransferableanonymous credentials with optionalanonymityrevocation", In:EUROCRYPT, 2001

Authors:

.

M.Rajya Lakshmi pursing M.Tech in Computer Science from **Sri Indu Institute of Engg.& Tech,Sheriguda(Vi),IBP(M),RR Dist.**

V.Ramesh working as Assistant professor, Department of CSE in **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi),IBP(M),RR Dist.**

Dr. I.Satyanarayana Completed B.E-Mechanical Engg. from Andhra University, M.Tech Cryogenic Engg. Specilization-IIT Kharagpur, Ph.D-Mechanical Engg.-JNTUH, Currently working as an Principal at **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi), IBP(M),RR Dist.**