ISSN:2320-0790

An International Journal of Advanced Computer Technology

Secured Data on Cloud Environment by SAPA Protocol with Auto-renewal

K. Prashanthi[1], P. Sangamithirai[2], S.Pothumani[3]

[1,2] B.Tech Student(CSE), Bharath University, Chennai-73.
[3,]Assistant Professor, Dept of CSE, Bharath University, Chennai-73

Abstract: Cloud computing is rising as a rife knowledge interactive paradigm to understand users' knowledge remotely hold on in a web cloud server. Cloud services offer nice conveniences for the users to relish the on-demand cloud applications while not c Knowledge Obstructity, Forward Security, Universal Composability onsidering the native infrastructure limitations. Throughout the information accessing, completely different users could also be in a very cooperative relationship, and so knowledge sharing becomes vital to attain productive edges. The prevailing security solutions chiefly concentrate on the authentication to understand that a user's privative knowledge cannot be unauthorized accessed, however neglect a delicate privacy issue throughout a user.It is difficult for the cloud server to request different users for knowledge sharing. The challenged access request itself might reveal the user's privacy in spite of whether or not it will acquire the information access permissions. During this paper, we have a tendency to propose a shared authority primarily based privacy-preserving authentication protocol (SAPA) to deal with higher than privacy issue for cloud storage. Within the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy concerns (e.g., authentication, knowledge obscurity, user privacy, and forward security); 2) attribute primarily based access management is adopted to understand that the user will solely access its own knowledge fields; 3) proxy re-encryption is applied by the cloud server to supply knowledge sharing among the multiple users. Meanwhile, universal compos ability (UC) model is established to prove that the SAPA on paper has the planning correctness. It indicates that the projected protocol realizing privacy-preserving knowledge access authority sharing is enticing for multi-user cooperative cloud applications.

Keywords: Knowledge Obstructity, Forward Security, Universal Composability

I. INTRODUCTION

The biggest challenge faced by an organization is to maintain and manipulate database.90% of the world data are created only within the last 2 years. Every sector today is gradually yet constantly moving towards electronic data management. So addressing them must take greater effort and precision. There are many number of data-storage and data-management tools available today but many of them lack the features like resource sharing and strong security with a complete cloud access solution. There are scenarios today, where an organization requires secured cloud storage where the entire participants in that organization can collaborate, with respect to their level of access. We present a cloud application that acts as a one-stop solution for the challenges mentioned above.

An organization can install this application in their network and include branches/ users, thereby creating an environment for the users to collaborate with the resources with respect to their level of access. We provide an additional security level, which we call as **User Level Access (ULA)**, which specifies the access rights over the resources. At any instance the user can only access the files under his level of **ULA**.

When a user requires data from the cloud, a simple search will result all the possible files containing the information. The user can then choose a file from the listed resources and request permission to the respective owner of the file. The request is then sent to the respective file owner via E-mail and also as a notification to the owner's dashboard.

The file owner can now choose either to grant permission or deny. If the permission is granted permission token is sent to the user who requested the file. The requested user will have to enter a special 4 digit Secured PIN (S-PIN) to download the file. Since this Application is running on a cloud server it become so convenient for the users to access the resources.

II. RELATED WORK

Paper 1 deals with Cloud based mostly information storage systems have several complexities relating to critical/confidential/sensitive information of consumer. to beat this drawback the paper handles key queries of the User regarding however information is uploaded on Cloud, maintained on cloud in order that there's no information loss; information is on the market to solely licensed User(s) as per Client/User demand and information recovery on disaster is applied. To maximize the storage potency and audit performance, general fragment structure into our audit system for outsourced storage. It permits owner of data to source their sensitive data to a Cloud Service Provider, and perform full block- level dynamic operations on the outsourced knowledge, i.e., block modification, insertion, deletion Authentication and authorization. Build common trust between the information owner and Cloud service Providers.

Paper 2 provides a secure access management in cloud computing. To supply a lot of secured access management it adopts a data structure and it uses a clock. Mistreatment this we are able to simply transfer, download, delete files from and to the cloud. Using this technique they mistreatment KP-ABE (Key Policy Attribute primarily based Encryption) and PRE (Proxy Re-Encryption).Owing to the overhead of coding and decoding. This technique isn't climbable. Each the house owners and therefore the users as cloud user.

For every cloud users our system keeps associate degree attribute set that contains a group of attributes similar to every user. It should vary with the user. A site contains several ranges of cloud users and one domain authority. Conjointly we have a tendency to use a clock to come up with the key with time.

Paper 3 deals with an economical and secure protocol to handle these problems. Our style relies on Elliptic Curve Cryptography and Sobol Sequence (random sampling). Our technique permits third party auditor to sporadically verify information the information integrity hold on at CSP while not retrieving original data. The existing schemes aim to providing integrity verification for various knowledge storage systems; however downside of confidentiality of information has not been absolutely addressed. An economical and secure protocol to make sure the confidentiality and integrity of knowledge storage in cloud computing mistreatment Elliptic Curve Cryptography (ECC) and Sobol Sequence.

Paper 4 deals with the tendency to discuss the drawbacks of approaches supported standard science techniques in addressing such downside so gift 2 approaches that address these drawbacks with totally different trade-offs. 1. A brand new Approach to manage cluster codingkeys a pair of. Basic approach to privacy conserving ABAC. It approaches addresses 2 requirements: Protective information confidentiality from the cloud; imposing fine-grained access management policies with relevancy the information users. The idea is to come up with associate ACV-BGKM instance for every attribute and mix the instances along mistreatment associate access structure that represents the attribute primarily based access management policy.

Paper 5 propose a secure multi-owner attribute authorities based mostly information sharing theme for dynamic teams within the cloud. Secure information sharing in an exceedingly dynamic cluster wherever the there's no fastened Attribute authorities wherever as multi – owner attribute authorities theme is feasible. Key policy attribute-based secret writing (KP-ABE) methodology is employed to pick out dynamic AA (Attribute authorities).Planning associate economical and secure knowledge sharing theme for teams within the cloud isn't a straightforward task attributable to the subsequent difficult problems.

a) Identity

b) It's counseled that any member in a bunch ought to be able to totally fancy the data storing and sharing services provided by the cloud, which is outlined because the multiple-owner manner. Compared with the single-owner manner

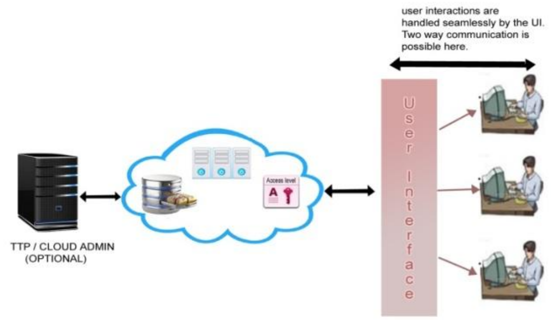
c).Member revocation and signed receipt. The user within the cluster will share and store knowledge files with others by the cloud; the complexness and size taken for secret writing is freelance with the quantity of revoked users in the system; User revocation may be achieved while not change the non-public keys of the remaining users and signed. Receipts are going to be collected when any revocation that reduces duplication of encrypted copies.

Paper 6 offers effective mechanism to trace usage of information victimization responsibility. Responsibility is checking of authorization policies and it\'s necessary for clear information access. Cloud provides three service models, beneath the information as a service, this is often having four components that are as per mentioned below, a).Encryption and decipherment - For security purpose of information hold on in cloud, cryptography looks to be excellent security answer. b)Key Management - If cryptography is critical to store knowledge within the cloud, cryptography keys can't be store there, therefore user needs key management. c) Authentication - For accessing hold on knowledge in cloud by licensed users. d) Authorization – Rights given to user still as cloud supplier. Accountability is important for observance knowledge usage, during this all actions of users like causation of file are cryptographically connected to the server, that performs them and server maintain secured record of all the actions of past and server will use the past records to understand the correctness of action. It conjointly provides reliable data concerning usage of knowledge and it observes all the records, thus it helps in create trust, relationship and name.

Paper 7 proposes that enabling public audit ability for cloud storage is of crucial importance so users will resort to a 3rd party auditor (TPA) to examine the integrity of outsourced information and be worry-free. We tend to propose a secure cloud storage system supporting privacy-preserving public auditing. We tend to additional extend our result to change the TPA to perform audits for multiple users at the same time and with efficiency. In our model, on the far side users' reluctance to leak information to TPA, we have a tendency to additionally assume that a cloud server has no incentives to reveal their hosted information to external parties. On the one hand, there are a unit rules. The system handles the following activities: They are: a)Notation and Preliminaries b) Definitions and Framework c) The Basic Scheme Privacy-Preserving Public Auditing theme. d)Support for Batch Auditing e) Support for information Dynamics. f) Generalization.

Paper 8 deals with the concentration on the authentication to appreciate that solely a legal user will access its licensed information, that ignores the case that completely different users might want to access and share every other's licensed information fields to realize productive advantages. Once a user challenges the cloud server to request alternative users for information sharing, the access request itself might reveal the user's privacy despite whether or not or not it will acquire the info access permissions. during this work, we tend to aim to deal with a user's sensitive access need connected privacy throughout information sharing within the cloud environments, and it's important to style a humanistic security theme to at the same time come through information access management, access authority sharing, and privacy preservation. It is revitalizing the accounts by responsive some security queries (These security question's answers square measure registered whereas registration) &amp; match the answers with answers that have uploaded earlier within the information base. These modules square measure created for privacy of Accounts. We address the aforesaid privacy issue to propose a shared authority based mostly privacy conserving authentication protocol (SAPA) for the cloud information storage that realizes authentication and authorization while not compromising a user's non-public data. The main contributions square measure as follows. a)Identify a brand new privacy challenge in cloud storage, and address a refined privacy issue throughout a user difficult the cloud server for information sharing, during which the challenged request itself will not reveal the user's privacy notwithstanding whether or not or not it can get the access authority. b) Propose associate authentication protocol to boost a user's access request connected privacy, and therefore the shared access authority is achieved by anonymous access request matching mechanism. c) Apply cipher text-policy attribute based mostly access management to comprehend that a user will dependably access its own information fields, and adopt the proxy re-encryption to produce temporary worker licensed information sharing among multiple users.

III. ARCHITECTURE DIAGRAM


user interactions are handled seamlessly by the UI. Two way communication is possible here.
User Interface
Access level
TTP / CLOUD ADMIN (OPTIONAL)

1. User Registration

A new user requiring an access for the cloud services should go through the registration phase to be a part of it. These details are maintained safely in a Database.

2. User Login

A secure user login module provides the application a base for the start of security through out. User has to enter his registered User Name and Password to login.

3. Dashboard

Dashboard is a special and an important module of the application where the users can maintain and share the resources accordingly.Following are the controls for managing the resources

A. Files

This section in the dashboard lists all the files that the logged in user has uploaded. The user can choose to share download or delete the files.

B. Share

This section in the dashboard lists all the files that are shared with the logged in user. The user can choose to share, download or delete the files.

C. Request

This section in the dashboard lists all the files that are owned by the user and are being requested by any other users on the cloud. The user can choose either to grant permission or deny/delete the request.

D. Settings

This section is used to manage the password, email information and the S-Pin of the logged in user.

4. Upload

In this module users can upload a file (along with meta data) into database, with the help of this metadata and its contents, the other users can search and request access to download the file. The uploaded file will be encrypted and only the registered users can access it except for the other users who have access permission granted by the file owner.

5. Cloud Server

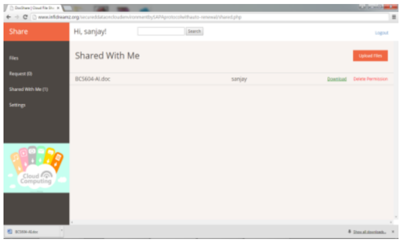
Cloud Server acts as the medium that connects the file storage system and the user level access control over them. It also plays role in validation and data security. All the data transactions are logged in the cloud server and hence every transaction is processed through the cloud server.

6. TTP(optional)

Any other external rules or implementations over the existing models can be easily designed by a cloud admin. This way an organization can truly achieve a complete cloud recourse sharing system with user level customization.

IV. IMPLEMENTATION

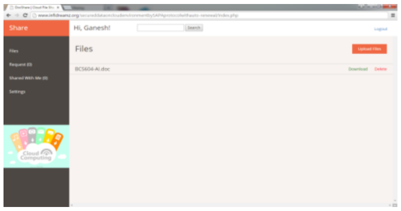
This architecture is implemented by using html ,Css and PHP.MY SQL is act as a database. Screen shots of File download; File upload, how the request are sent and how the request found are shown in the following figures:



Shared With Me

BCS604-AI.doc sanjay

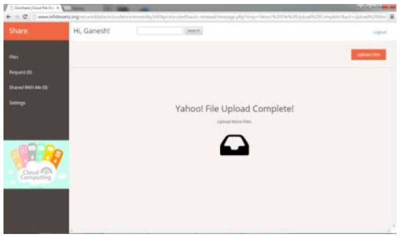
File Download



Files

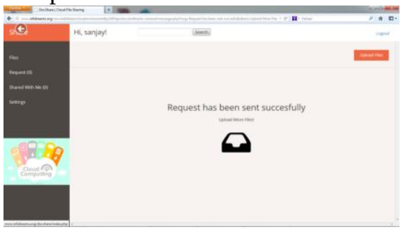
BCS604-AI.doc

File upload1



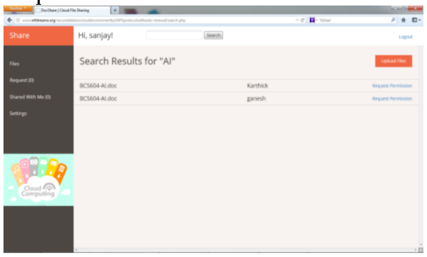
Yahoo! File Upload Complete!

File upload



Request has been sent succesfully

Request sent



Search Results for "AI"

BCS604-AI.doc Karthick

BCS604-AI.doc ganesh

Request found

V. CONCLUSION

In this work, we've known a replacement privacy challenge throughout information accessing within the cloud computing to attain privacy-preserving access authority sharing. Authentication is established to ensure information confidentiality and information integrity. Information obscurity is achieved since the wrapped values ar changed throughout transmission. User privacy is increased by anonymous access requests to in camera inform the cloud server regarding the users' access needs. Forward security is completed by the session identifiers to forestall the session correlation. It indicates that the projected theme is probably applied for increased privacy preservation in cloud applications.

VI. REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology,USA, 2009.

[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," *IEEE Communications Magazine*, vol. 50, no. 9, pp, 24-25, 2012.

[3] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente,"Key Challenges in Cloud Computing to Enable the Future Internet of Services," *IEEE Internet Computing*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, 2012.

[4] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol. 14,no. 5, pp. 14-22, 2010.

[5] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," *Computer*, vol. 45, no. 7, pp. 73-78,2012.

[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, "Proxy Provable Data Possession in Public Cloud-s," IEEE Transactions on Services Computing, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[8] K. Yang and X. Jia, "An Efficient and Secure Dynamic Au-diting Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[10] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, 2010.

[11] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[12] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.