MUTUAL KEY OVERSIGHT PROCEDURE FOR CLOUD SECURITY AND DISTRIBUTION OF DATA BASED ON HIERARCHY METHOD

M. Rekha[1], Mr. Sathish Kuumar[2]

[1]Student, [2]Assistant Professor

Department Of Computer Science and Engineering

Gojan School Of Business and Technology, Redhills, Chennai.

ABSTRACT-*Meanwhile, cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Access control is paramount as it is the first line of defense that prevents unauthorized access to the shared data. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to- end data confidentiality assurance in the cloud and beyond. Clients risk key exposure that is hardly noticed but inherently existed in previous research. Furthermore, enormous client decryption overhead limits the practical use of ABE. The proposed collaborative Mechanism effectively solves not only key escrow problem but also key exposure. Meanwhile, it helps markedly reduce client decryption overhead.*

However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying cipher text-policy, making the computation over encrypted data a very hard problem. The proposed scheme not only achieves scalability due to its hierarchical structure.

Keywords: **Hierarchical security, Cloud authority, Domain authority, Cipher-text, Attribute Based Encryption.**

1. INTRODUCTION

In cloud computing, authority accepts the user enrollment and creates some parameters. Cloud service provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated cipher-text to CSP. User downloads and decrypts the interested ciphertext from CSP. The shared files usually have hierarchical structure. That is, a department of files is divided into a number of hierarchy sub departments located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved. Presently a day's more number of plans utilized encryption for control the information in cloud. It empowers clients with restricted computational assets to outsource their expansive calculation workloads to the cloud, and monetarily appreciate the monstrous computational power, data transfer capacity, stockpiling, and even proper programming that can be partaken in a compensation for each utilization way. Distributed computing is a progressive registering worldview which empowers adaptable, on-request and minimal effort utilization of figuring assets. Those points of interest, unexpectedly, are the reasons for security and protection issues, which rise in light of the fact that the information claimed by various clients are put away in some cloud servers rather than under their own control. The security issue of distributed computing is yet to be settled. To manage security issues, different plans in light of the Attribute-Based Encryption have been utilized. From one perspective, the outsourced figuring workloads often contain sensitive information, for instance, the business money related records, prohibitive research data, or eventually identifiable prosperity information et cetera. To fight against unapproved information spillage, sensitive data must be mixed before outsourcing so as to offer end to-end data protection affirmation in the cloud and past.

Regardless, normal data encryption procedures by and large shield cloud from playing out any critical operation of the essential figure content game plan, making the count over encoded data a troublesome issue. The proposed plot not simply achieves flexibility due to its dynamic structure. We give the protection secure out in the open social distributed computing. In our venture we actualize progressive property base security the pecking orders are Cloud specialist, Domain expert and clients. Cloud expert can just have benefit to make or expel the domain (private cloud specialist) in cloud and they can keep up every one of the points of interest in general cloud Domain expert can make or evacuate the clients inside the area this clients are called private clients. Clients are two sorts private cloud client and open cloud client's Private cloud clients are depends the space Public clients under cloud specialist. Clients can transfer the documents in two ways: Public and Private. On the off chance that the private client transfer general society document, the record perceivability and availability is just inside area itself and same space clients can get to that document with no security validation If the general population client transfer people in general document, the record perceivability and openness is constantly open any cloud client can get to that document. For Private transfer If private client transfer the private document implies that record perceivability is just inside space yet document openness is who have the emit key (OTP) implies who have benefit to get to the record If general society client transfer the private document implies that document perceivability is open anybody can obvious the document yet who have a benefit (OTP) to get to they just can get to the document.

2. EXISTING SYSTEM

The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. The hierarchy structure of shared files hasn't been explored in CP-ABE. Using Cipher text-policy attribute based encryption to secure the cloud storage part.The authority for file access control in which authorized of all operations on cloud data can be managed in the entire manner.The key authority must be completely trustworthy, as it can decrypt all the cipher text using generated private key without permission of its owner.To avoid unauthorized information leakage, sensitive data have to be encrypted before outsourcing. Role based encryption is used for encrypting the data based on the authority provided .

3. RELATED WORKS

In this paper the cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE)by extending cipher text-policy attribute-set-based encryption(ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bettencourt et al. and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments [1]
In this paper with the rapid developments occurring in cloud computing and services, there has been a growing trend to use the cloud for large-scale data storage. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. One well known access control model is the role-based access control (RBAC), which provides flexible controls and management by having two mappings, users to roles and roles to privileges on data objects. In this paper, we propose a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. Our RBE scheme allows RBAC policies to be enforced for the encrypted data stored in public clouds. Based on the proposed scheme, we present a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. We describe a practical implementation of the proposed RBE-based architecture and discuss the performance results. We demonstrate that users only need to keep a single key for decryption, and system operations are efficient regardless of the complexity of the role hierarchy and user membership in the system[2]

Secure cloud storage solutions such as Trust Store, SecCloud, HPI Secure, and Twin Cloud have primarily focused on securing persistent data while storing it in public cloud services. Though data sharing has been recognized as an important security feature, these storage solutions mostly focus on three key properties: confidentiality, integrity and availability. Modern enterprise applications demand data is able to be shared within or across organizations. The challenges how to securely share data in public clouds without increasing data movement and computation costs. This problem has been addressed in recent times by utilizing or developing new data encryption techniques such as identity-based encryption, attribute-based encryption and proxy-re-encryption. However, these techniques suffer from scalability and flexibility problems when dealing with big data and support for dynamic access control rules. This paper presents a novel architecture and corresponding protocols to provide secure sharing of document son public cloud services: CloudDocs. This system uses AES fordata encryption to achieve scalability and supports identity based access control rules using private-public key pairs to provide flexibility[3]

In this works more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, selectively can be shared only at a coarse-grained level (i.e., giving another party your private key). fine-grained sharing can develop a new cryptosystem of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are consists with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. To demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE)[4].

As more sensitive data can be shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). Fine-grained sharing can new cryptosystem of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE)[5]

4. PROPOSED SYSTEM

We offer the security of social cloud computing. In this paper we put into practice hierarchical security, Cloud authority, Domain authority and users. Cloud authority can only have a privilege to create or remove the province in cloud and they can preserve all the details in overall cloud Domain authority can create or eliminate the users contained by the domain this users are called private users . Two type users will be there. One is private cloud user and another one is public cloud users. Private users are reply on the domain, Public users under cloud authority. User has a two way of uploading files Public and Private. If one file uploaded by private user, file visibility and convenience having only within domain without confirmation. If some file should uploaded by public user's then, file access privileges having all the users. To enhance both security and efficiency of key management in cipher text policy attribute-based encryption for cloud data sharing system.If file uploading the private user means file visibility is only within field but file accessibility is who have the secrete key (OTP) means who have license to access the file If the public user upload the private file means that file visibility is public anyone can noticeable the file but who have a privilege like one time password to access they only can access the file [4].

5. SYSTEM DESIGN FOR DISTRIBUTION OF DATA

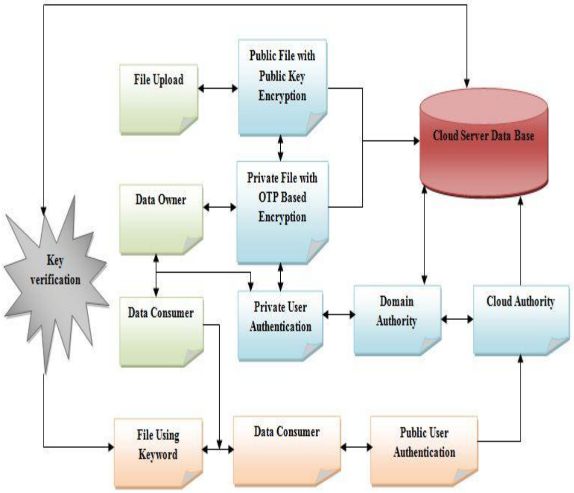


fig-1: proposed architecture

6. SYSTEM IMPLEMENTATION

MODULES:

- *Data Owner*
- *Data Consumer*
- *Domain level Security*
- *Attribute based security*
- *Secret file accessing*

7. MODULES DESCRIPTION

7.1 DATA OWNER

In this module, the data owner uploads the data in the cloud server. For the security purpose the data owner encrypts the data file and then store in to the cloud. The data owner can change the policy over data files by updates the expiration time. The Data owner can have to capable of manipulate the encrypted data file. The data owner can be set the access privilege to the encrypted data file. Data owner to delegate most of the computational overhead to cloud servers. The KP-ABE used to provides fine-grained access control gracefully. Each file is encrypted with a symmetric data encryption key ( ), which is in turn encrypted by a public key corresponding to a set of attributes in KP-ABE, which is generated according to an access structure. The encrypted data file is stored with the corresponding attributes and the encrypted. If the associated attributes of a file stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted, which is used turn to decrypt the file. 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. Each data owner consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner.

7.2 DATA CONSUMER

The user can be only access the data file with the encrypted key if the user have to privilege to access the file. For the user level, the Domain authority are given all the privileges and the Data user's are controlled by the Domain Authority only. Users can be able to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. Data owners encrypt their data files and then store them in to the cloud for sharing with data consumers. To access the shared data files, data consumers and download encrypted data files of their interest from the cloud and then decrypt them. Domain authority is administrated each data owner/consumer. A domain authority is managed by the parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. data consumers will be always online. They come online only when necessary, while the cloud service provider, the trusted authority, and domain authorities are always online. The cloud is assumed to have abundant storage capacity and computation power. In addition, we assume that data consumers can access the data files for reading purpose only.
Data consumer create the account and then login to access the cloud storage information and data consumer entry level based on the hierarchical manner.

7.3 DOMAIN SECURITY LEVEL

The trusted authority acts the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users administrates, but try to get the private keys of users outside its domain. Users cab able to access data files either within or outside the scope of their access privileges, so malicious users can collude with each other to get sensitive files beyond their privileges. we assume that communication channels between all the parties are secured by using standard security protocols.
Domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. Each top-level domain authority corresponds to a top-level organization, such as a federated enterprise, while each lower-level domain authority corresponds to a lower-level organization, such as an affiliated company in a federated enterprise. Data owners/consumers may correspond to employees in an organization. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain.
Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. System model consists of a trusted authority, multiple domain authorities, and numerous users corresponding to data owners and data consumers. The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.

7.4 ATRIBUTE BASED SECURITY:

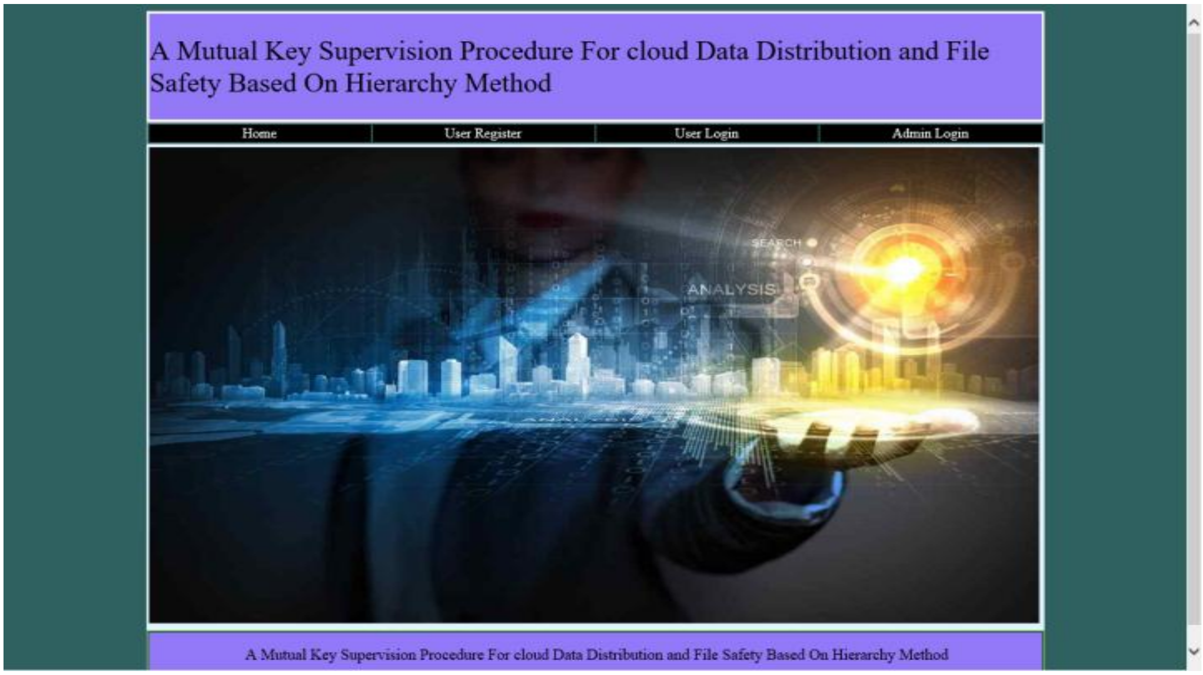
The HASBE scheme seamless incorporates a hierarchical structure of system users by apply to delegation algorithm to ASBE. HASBE not supports compound attributes due to the flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. We can proved the security of HASBE based on the security of CP-ABE. A hierarchical attribute-set-based encryption (HASBE) scheme can be access control in cloud computing. HASBE extends the cipher text-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

7.5 SECRET FILES ACCESSING

Fig 1 shows the concept of the cloud service provider manages a cloud to provide data storage service. Data owners can encrypt their data files and store them in to the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of the interest from the cloud domain and then decrypt them. The cloud server provider is entrusted in the sense that it may collude with malicious users (short for data owners/data consumers) to harvest file contents stored in the cloud for its own benefit. In the hierarchical structure of the system users given in each party is associated with a public key and a *private key, with the latter being kept secretly by the party. Users can be able to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. The traditional methods to protect the sensitive data outsourced to third parties is to store encrypted data on servers, while the decryption keys are disclosed to authorize users only.*

8. SCREEN SHOTS

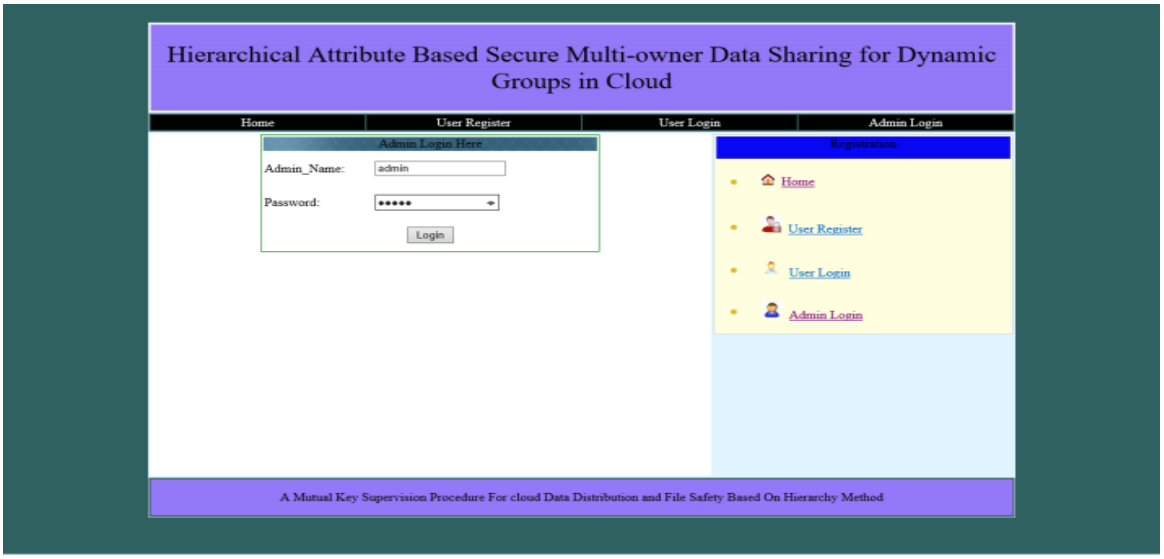
HOME PAGE



A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

ADMIN LOGIN



Hierarchical Attribute Based Secure Multi-owner Data Sharing for Dynamic Groups in Cloud

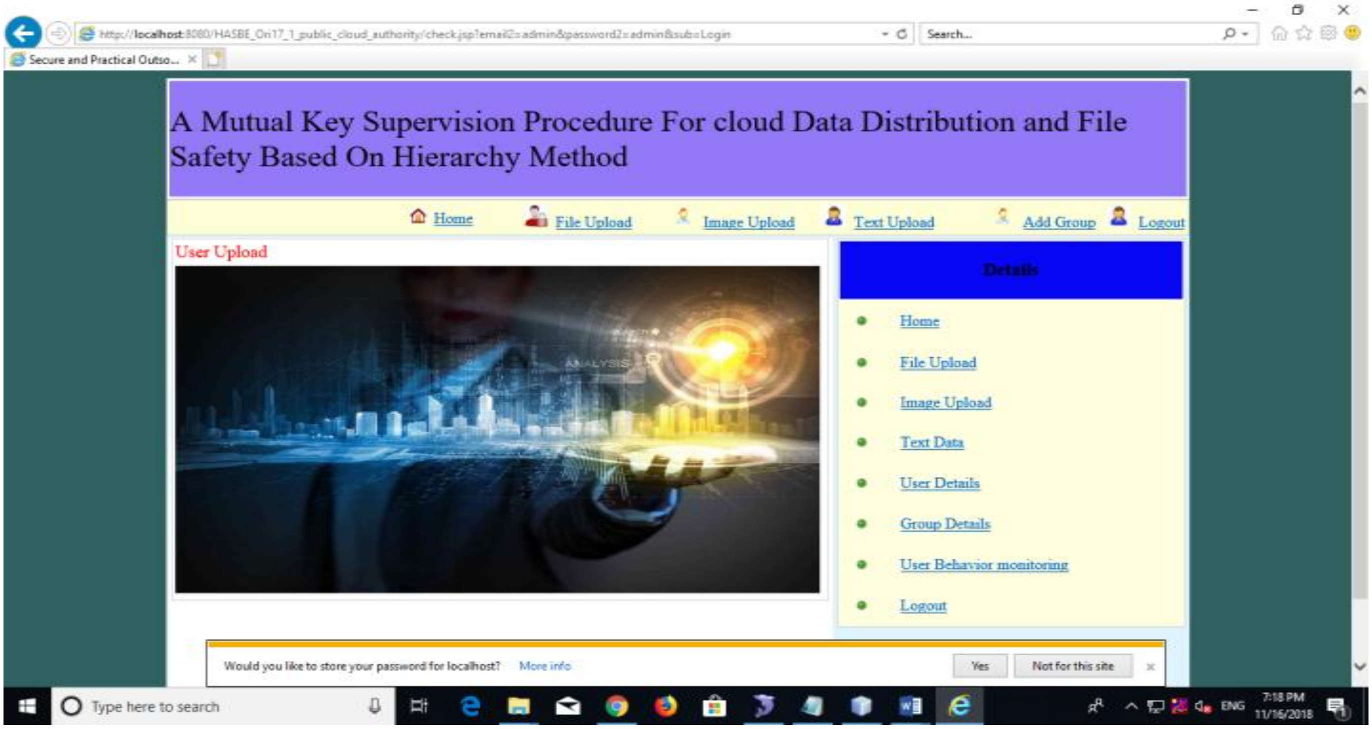
Admin Login Here

Admin_Name: admin

Password: •••••

A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

ADMIN PAGE



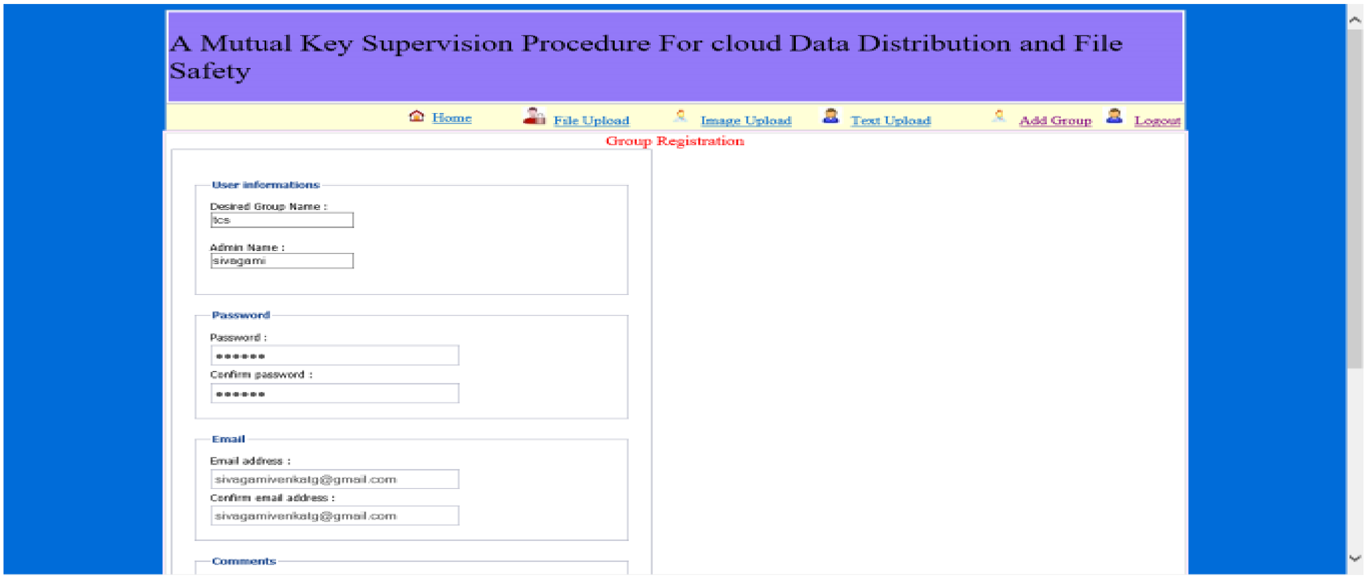
http://localhost:8080/HASBE_Ori17_1_public_cloud_authority/check.jsp?email2=admin&password2=admin&sub=Login

A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

User Upload

Would you like to store your password for localhost?

USER REGISTER:



A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety

Group Registration

User informations

Desired Group Name : tcs

Admin Name : sivagami

Password

Password : ●●●●●●

Confirm password : ●●●●●●

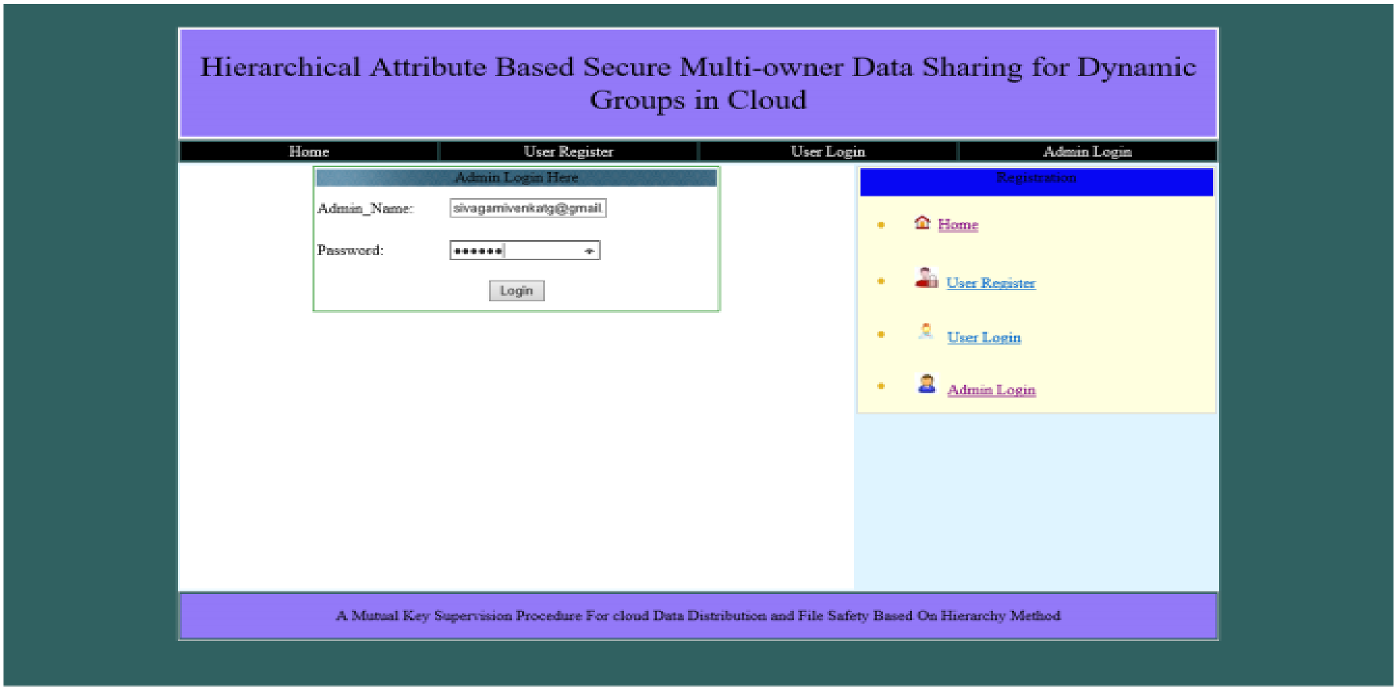
Email

Email address : sivagamivenkatg@gmail.com

Confirm email address : sivagamivenkatg@gmail.com

Comments

USER LOGIN PAGE



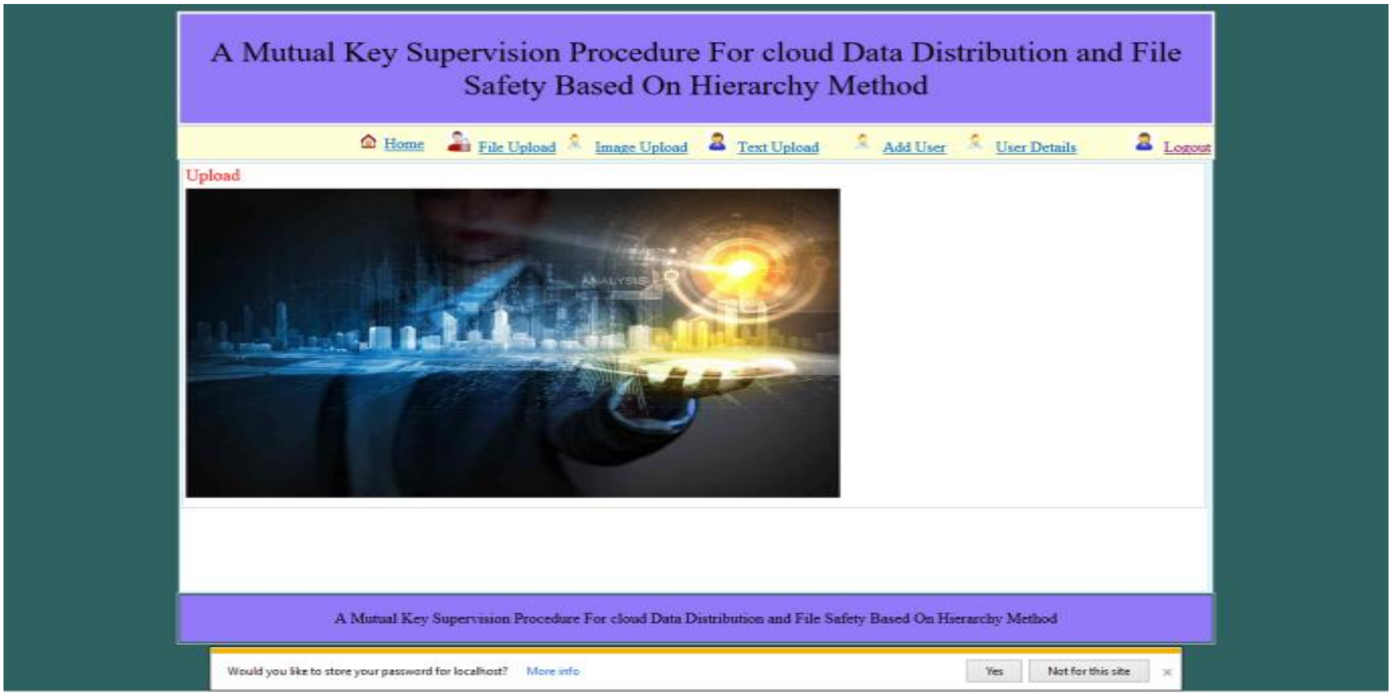
Hierarchical Attribute Based Secure Multi-owner Data Sharing for Dynamic Groups in Cloud

Admin_Name: sivagamivenkatg@gmail

Password: ••••••

A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

USER PAGE

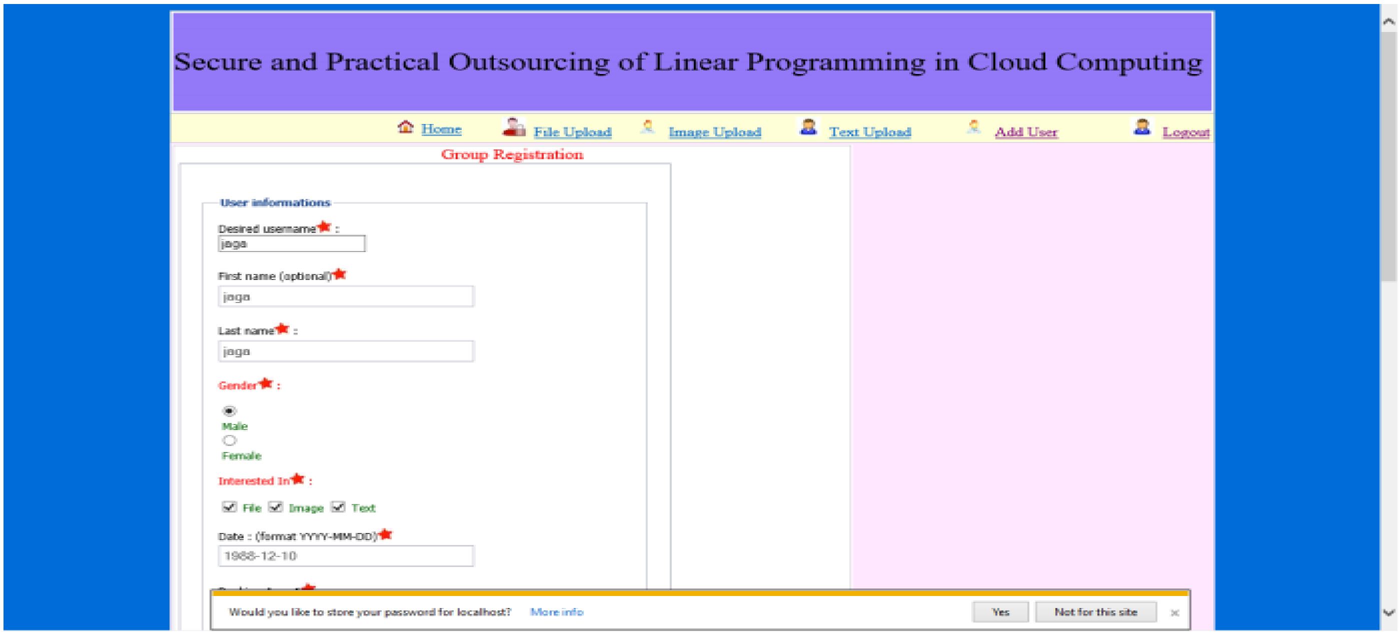


A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

A Mutual Key Supervision Procedure For cloud Data Distribution and File Safety Based On Hierarchy Method

Would you like to store your password for localhost? More info

GROUP REGISTERATION



Secure and Practical Outsourcing of Linear Programming in Cloud Computing

Group Registration

User informations

Desired username* : jaga

First name (optional)* jaga

Last name* : jaga

Gender* :

● Male
○ Female

Interested In* :

☑ File ☑ Image ☑ Text

Date : (format YYYY-MM-DD)* 1988-12-10

Would you like to store your password for localhost?

9. CONCLUSION

A semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities by using cloud computing system and our proposed schemes achieve is not only fine-grained privilege control is also identity anonymity while conducting the privilege control based on users' identity information. More importantly in our system can be tolerate up to N – 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment.

FUTURE ENHANCEMENTS

Future enhancement of this project is following schemes. A unified scheme is used for resource protection in automated trust negotiation. Automated trust negotiation using cryptographic credentials.

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng,
"A HIERARCHICAL ATTRIBUTE-BASED SOLUTIONFOR FLEXIBLE AND SCALABLE ACCESS CONTROLIN CLOUD COMPUTING", 2012.
[2] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "ACHIEVING SECURE ROLE-BASED ACCESS CONTROL ON ENCRYPTED DATA IN CLOUD STORAGE", 2015.
[3] Catherine Wise, Carsten Friedrich, Surya Nepal, Shiping Chen and Richard O. Sinnott.
"CLOUDDOCS: SECURE SCALABLE DOCUMENT SHARING ON PUBLIC CLOUDS
2015.
[4] VipulGoyal, OmkantPandey, AmitSahai and Brent Waters, "ATTRIBUTE-BASED ENCRYPTION FORFINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA2016
[5] John Bethencourt, AmitSahai, and Brent Waters, "CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTIO", 2017.