International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

# Control Cloud Data Access Privilege with Fully Anonymity

Mr.k.Sarangam ; P.Vandana ; S.Divya ; E.Mani Teja
(Assistant Professor), k.sarangam@hotmail.com , vandanapishke147@gmail.com
divyareddys125@gmail.com , mani.sunny321@gmail.com
[1,2,3,4,] Dept.of Computer Science and Engineering, Vignan Institute of Technology and Science, Vignan Hills, Deshmukhi Village, Nalgonda, Telangana, 508284

***Abstract:***

*Distributed computing is a progressive registering worldview, which empowers adaptable, on-request, and minimal effort utilization of figuring assets, however the information is outsourced to some cloud servers, and different security concerns rise up out of it. Different plans in view of the property based encryption have been proposed to secure the distributed storage. In any case, most work centers around the information substance protection and the entrance control, while less consideration is paid to the benefit control and the character security. In this paper, we exhibit a semi-unknown benefit control conspire Anony Control to address the information security, as well as the client character protection in existing access control plans. Anony Control decentralizes the focal specialist to restrain the character spillage and in this way accomplishes semi-namelessness .Besides, it likewise sums up the document get to control to the benefit control, by which benefits of all tasks on the cloud information can be overseen in a fine-grained way. Along these lines, we display the Anony Control-F, which completely keeps the personality spillage and accomplish the full namelessness. Our security examination demonstrates that both Anony Control and Anony Control-F are secure under the decisional bilinear Diffie– Hellman supposition, and our execution assessment shows the achievability of our plans.*

***Keywords***

*Anonymity, multi-authority, attribute-based encryption.*

## 1. Introduction

Distributed computing gives huge patterns in the present IT world. Because of the advantages…. it gives consideration on business, industry and additionally the scholarly world.

It gives registering assets progressively by means of Internet. However, has a few difficulties related, similar to information secrecy, information protection and security.

Security is identified with the information substance and the clients character, so it is have to ensure the personality of clients.

The objective of distributed computing is to apply conventional supercomputing, or superior registering power, regularly utilized by military and research offices, to perform several trillions of calculations for every second, in shopper arranged applications, for example, money related portfolios, to convey customized data, to give information stockpiling or to influence expansive, immersive PC amusements.

The distributed computing utilizes systems of vast gatherings of servers normally running ease purchaser PC innovation with specific associations with spread information handling errands crosswise over them. This common IT foundation contains expansive pools of frameworks that are connected together. Regularly, virtualization strategies are utilized to augment the energy of distributed computing.

The notable attributes of distributed computing in light of the definitions gave by the National Institute of Standards and Terminology (NIST) are laid out underneath:

- On-request self-benefit: A customer can singularly arrangement registering capacities, for example, server time and system stockpiling, as required naturally without requiring human connection with each specialist co-op's.
- Broad organize get to: Capabilities are accessible over the system and got to through standard instruments that advance use by heterogeneous thin or thick customer stages (e.g., cell phones, workstations, and PDAs).
- Resource pooling: The supplier's figuring assets are pooled to serve various buyers utilizing a multi-occupant display, with various physical and virtual assets progressively doled out and reassigned by shopper request. There is a feeling of area autonomy in that the client by and large has no control or information over the correct area of the gave assets yet might have the capacity to determine area at a larger amount of reflection (e.g., nation,

state, or server farm). Cases of assets incorporate capacity, handling, memory, organize transfer speed, and virtual machines.

• Rapid flexibility: Capabilities can be quickly and flexibly provisioned, now and again consequently, to rapidly scale out and quickly discharged to rapidly scale in. To the purchaser, the capacities accessible for provisioning regularly seem, by all accounts, to be boundless and can be bought in any amount whenever.

• Measured benefit: Cloud frameworks naturally control and improve asset use by utilizing a metering capacity at some level of deliberation proper to the sort of administration (e.g., capacity, handling, transfer speed, and dynamic client accounts). Asset use can be overseen, controlled, and detailed giving straightforwardness to both the supplier and purchaser of the used administration.

To outline and execute a multi expert completely unknown Attribute Based Encryption control plan to address the information protection and client personality security issues in distributed computing condition.

On-request self-benefit: A purchaser can singularly arrangement registering abilities, for example, server time and system stockpiling, as required consequently without requiring human collaboration with each specialist co-op's.

Expansive system get to: Capabilities are accessible over the system and got to through standard components that advance use by heterogeneous thin or thick customer stages (e.g., cell phones, PCs, and PDAs).

Asset pooling: The supplier's figuring assets are pooled to serve numerous shoppers utilizing a multi-occupant display, with various physical and virtual assets powerfully appointed and reassigned by buyer request. There is a feeling of area autonomy in that the client for the most part has no control or information over the correct area of the gave assets however might have the capacity to determine area at a more elevated amount of reflection (e.g., nation, state, or server farm). Cases of assets incorporate capacity, preparing, memory, organize transfer speed, and virtual machines.

Fast versatility: Capabilities can be quickly and flexibly provisioned, at times naturally, to rapidly scale out and quickly discharged to rapidly scale in. To the customer, the capacities accessible for provisioning frequently give off an impression of being boundless and can be obtained in any amount whenever.

Estimated benefit: Cloud frameworks naturally control and improve asset use by utilizing a metering capacity at some level of deliberation suitable to the kind of administration (e.g., capacity, preparing, transfer speed, and dynamic client accounts).

The Data Access control is given to the customer to the restricted access to the cloud for the execution and utilization of the cloud.

The examination has some confinement as takes after: Difficult to client repudiation. At whatever point a proprietor needs to change the entrance right of the client, it isn't conceivable to do effectively. Decoding keys just help client properties which are composed sensibly as a solitary set, so clients can simply utilize every single conceivable mix of attributes in an extraordinary set issued in their keys to fulfill the strategies.

There has been a huge turnover of workers in associations managing data frameworks because of the dynamic idea of callings and security data itself (Karabacak and Sogukpinar, 2005). Turnovers of security and arrangement masters can prompt antagonistic misfortunes of pivotal data. In the current years, the picture of the corporate to individuals has experienced a striking change

The data security callings and the data framework assume a basic part in information uprightness and the general accomplishment of an association. The data innovation industry depends essentially on the high requirement for add up to security, secrecy and individual morals (Karabacak and Sogukpinar, 2005).

The notoriety of a firm may be destroyed if its technique of data security saw as inadmissible or insufficient. The headway in innovation makes it less demanding to break the 32 uprightness of data and is extremely hard to distinguish. For example, security and development insider facts can be effectively exchanged starting with one association then onto the next when faculty leaves starting with one organization then onto the next. It is, in this manner, extremely critical for an enterprise to be exceptionally enthusiastic about holding and enhancing its workers' aptitudes to bring down this condition.

Therefore, it is essential for organizations to realize that for the company to lower risks and improve security across the firm, it must place its priority on people who are the most valuable assets that can help the enterprise meet its diverse goals.

## 2. Literature Review

1) Attribute-based encryption for fine-grained access control of encrypted data:

AUTHORS: V. Goyal, O. Pandey, A. Sahai, and B. Waters

As 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 is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

2) Improving privacy and security in multi-authority attribute-based encryption:

AUTHORS: M. Chase and S. S. M. Chow Attribute based encryption (ABE) [13] determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority be-fore decrypting a message. Chase [5] gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users ' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

3) Secure threshold multi authority attribute based encryption without a central authority:

AUTHORS: H. Lin, Z. Cao, X. Liang, and J. Shao

An attribute based encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each cipher text. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open problem presented by Sahai and Waters in EUROCRYPT 2005. However, her scheme needs a fully trusted central authority which can decrypt every cipher text in the system. This central authority would endanger the whole system if it's corrupted.

This paper presents a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encryptor can encrypt a message such that a user could only decrypt if he has at least d k of the given attributes about the message for at least $t+1$, $t \leq n/2$ honest authorities of all the n attribute authorities in the proposed scheme. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme and be further extended to a proactive MA-ABE scheme.

4) Multi-authority attribute-based encryption with honest-but-curious central authority

AUTHORS:V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi

An attribute-based encryption scheme capable of handling multiple authorities was recently proposed by Chase. The scheme is built upon a single-authority attribute-based encryption scheme presented earlier by Sahai and Waters. Chase's construction uses a trusted central authority that is inherently capable of decrypting arbitrary cipher texts created within the system. We present a multi-authority attribute-based encryption scheme in which only the set of recipients defined by the encrypting party can decrypt a corresponding cipher text. The central authority is viewed as 'honest-but-curious': on the one hand, it honestly follows the protocol, and on the other hand, it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. The proposed scheme, which like its predecessors relies on the Bilinear Diffie–Hellman assumption, has a complexity comparable to that of Chase's.

5) Attribute-based secure data sharing with hidden policies in smartgrid

AUTHORS: J.Hur

Smart grid uses intelligent transmission and distribution networks to deliver electricity. It aims to improve the electric system's reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning. The smart grid systems use fine-grained power grid measurements to provide increased grid stability and reliability. Key to achieving this is securely sharing the measurements among grid entities over wide area networks. Typically, such

sharing follows policies that depend on data generator and consumer preferences and on time-sensitive contexts. In smart grid, as well as the data, policies for sharing the data may be sensitive because they directly contain sensitive information, and reveal information about underlying data protected by the policy, or about the data owner or recipients. In this study, we propose an attribute-based data sharing scheme in smart grid. Not only the data but also the access policies are obfuscated in grid operators' point of view during the data sharing process. Thus, the data privacy and policy privacy are preserved in the proposed scheme. The access policy can be expressed with any arbitrary access formula. Thus, the expressiveness of the policy is enhanced. The security is also improved such that the unauthorized key generation center or the grid manage systems that store the data cannot decrypt the data to be shared. The computation overhead of recipients are also reduced by delegating most of the laborious decryption operations to the more powerful grid manage systems.

## 3. System Analysis

***Existing System***

- Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it.

- Few years later, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE).

- The work by Lewkoet al. and Muller et al. are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones.

- Lewkoet al. use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to boolean formula, while we inherit the flexibility of the access tree having threshold gates.

- Muller et al. also supports only Disjunctive Normal Form (DNF) in their encryption policy.

***Disadvantages Of Existing System***

- The identity is authenticated based on his information for the purpose of access control (or privilege control in this paper).

- Preferably, any authority or server alone should not know any client's personal information.

- The users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

***Proposed System***

- The data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes.

- We propose Anony Control and Anony Control-Fallow cloud servers to control users' access privileges without knowing their identity information. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. The scheme proposed by Chase et al. considered the basic threshold-based KP-ABE .Many attribute based encryption schemes having multiple authorities have been proposed afterwards.

- In our system, there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and a Data Consumer simultaneously.

- Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N is joint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

***Advantages Of Proposed System:***

- The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F.

- The proposed schemes are tolerant against authority compromise, and compromising of up to (N −2) authorities does not bring the whole system down.

- We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F.

- We firstly implement the real toolkit of a multi authority based encryption scheme AnonyControl and AnonyControl-F.

Requirement analysis in system engineering and software engineering encompasses those tasks that go into determining the needs or conditions to meet for a new or alerted product, taking account of the

possibly conflicting requirements of the various stakeholders, such as beneficiaries or users.

Input design is a part of overall system design. The main objective during the input design is as given below:

- To produce a cost-effective method of input.
- To achieve the highest possible level of accuracy.
- To ensure that the input is acceptable and understood by the user.

Input stages:

- The main input stages can be listed as below:
  - Data recording
  - Data transcription
  - Data conversion
  - Data verification
  - Data control
  - Data transmission
  - Data validation
  - Data correction

Input types:

It is necessary to determine the several types of inputs.

Inputs can be categorized as follows:

- External inputs, which are prime inputs for the system.
- Internal inputs, which are user communications with the system.
- Operational, which are computer department's communications to the system?
- Interactive, which are inputs entered during a dialogue

Input media:

At this stage choice must be made about the input media.

To conclude about the input media consideration must be given to

- Type of input
- Flexibility of format
- Speed
- Accuracy
- Verification methods
- Rejection rates
- Ease of correction
- Storage and handling requirements
- Security
- Easy to use
- Portability

Keeping in view the above description of the input types and input media, it can be said that most of the inputs are of the form of internal and interactive.

Input data is to be the directly keyed in by the user, the keyboard can be considered to be the most suitable input device.

Output definition

The outputs should be defined in terms of the following points:

- Type of the output
- Content of the output
- Format of the output
- Location of the output
- Frequency of the output
- Volume of the output
- Sequence of the output.

It is not always desirable to print or display data as it is held on a computer. It should be

decided as which form of the output is the most suitable.

For Example

- Will decimal points need to be inserted?
- Should leading zeros be suppressed.

Output media:

In the next stage it is to be decided that which medium is the most appropriate for the output.

The main considerations when deciding about the output media are:

- The suitability for the device to the application.
- The need for a hard copy.
- The response time required.
- The location of the users

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

- The software and hardware available.

Keeping in view the above description the project is to have outputs mainly coming under the category of internal outputs. The main outputs desired according to the requirement specification are:

The outputs were needed to be generated as a hard copy and as well as queries to be viewed on the screen. Keeping in view these outputs, the format for the output is taken from the outputs, which are currently being obtained after manual processing. The standard printer is to be used as output media for hard copies.

## 4. System Design and Implementation

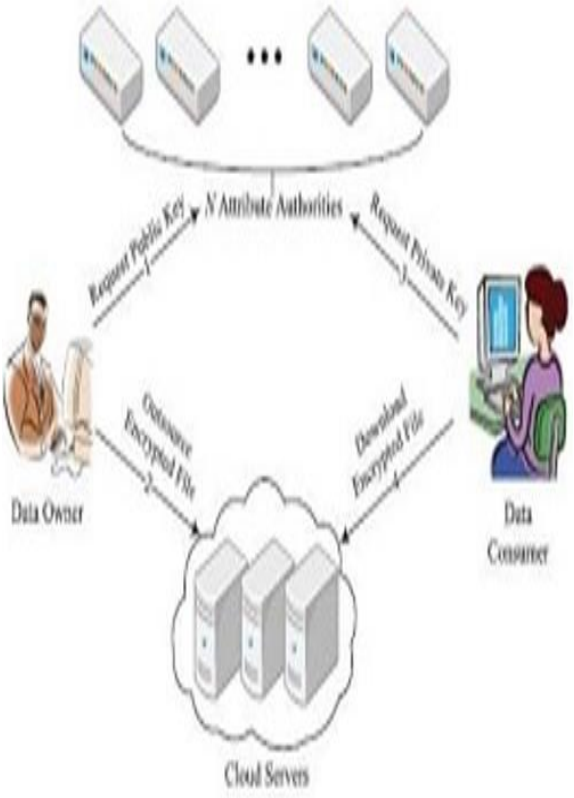



Fig 1: System Architecture

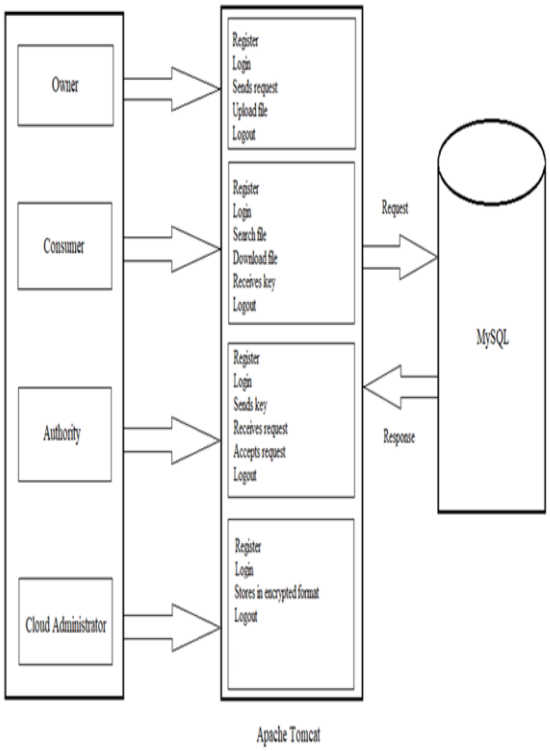



Fig 2: Data-Flow Diagram

***Modules Description***

A module description provides detailed information about its supposed components, which is accessible in different manners. The included description is available by reading directly, by generating a short html-description, or by making an environment check for supposed components to check if needed types and services are available in the environment where they will be used. This environment checks registration/installation or a separate consistency check for a component.

There are three ways Key Management can be effective:

▪ Securing key stores: The key stores is where the keys stored and created so high security protocols implanted in the key stores to protect them from malicious users. Gaining access to key means gaining the lead to the encrypted data associated to that key. Hence the key stores themselves are protected in storage, in transit and on backup media.

▪ Access to key stores: Access to the key stores limited to the users that have the rights to get access to data. Role authentication protocols to help control access. Key creation storing and retrieval owned by different entities with this approach the management becomes easy and in events of intrusion the cause to find and terminated quickly.

▪ Key backup and recoverability: Loosing a key means losing all the data associated to that key. Keys storage and backup solutions designed carefully. In

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

case of events where keys destroyed there must be recovery options placed so that data associated to that key is retrieved and again a new key is generated to encrypt the data.

There are four forms in the application. First one is the login form , second is the registration form , which must filled by the owner and the consumer while posting the free space in the application , third is the attribute authority and the last one is the cloud server.

## 5. Results and Analysis

**Public Key**: In this Module public key is generated for authentication for the user to provide the user specification logging.

**File Storage:** The File Storage module the file stored for the further usage of the consumer and the file is provided the option to view and Download based on the time period keys.

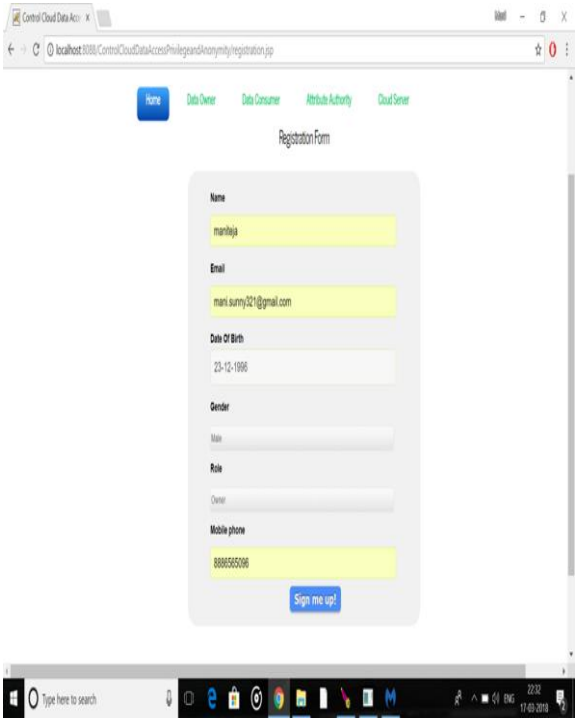
**Encryption:** The files are encrypted in order to provide security to the documents or the contents of the provider.

**Data Access Control:** The Data Access control is provided to the consumer for the limited access to the cloud for the performance and usage of the cloud.

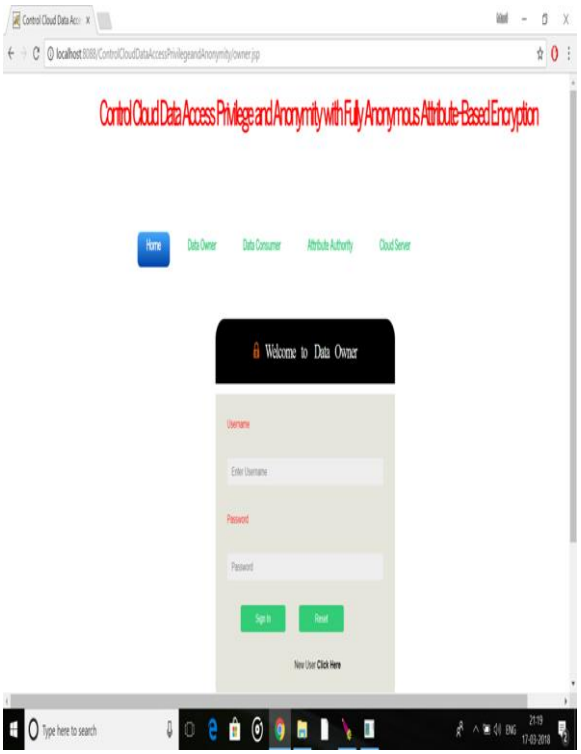
**Data Access:** The Data can be accessed by viewing the content of the file or downloaded for the further usage.

1) Home Page


2) Owner Registration

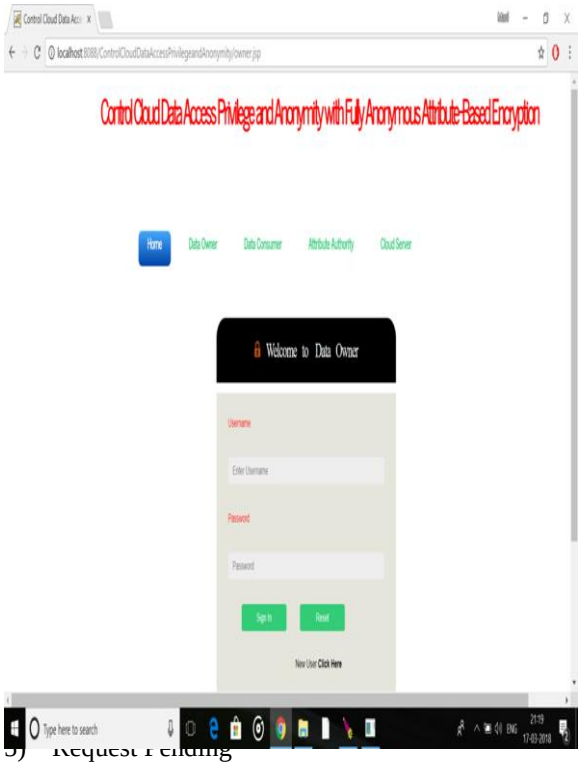



3) User Registration

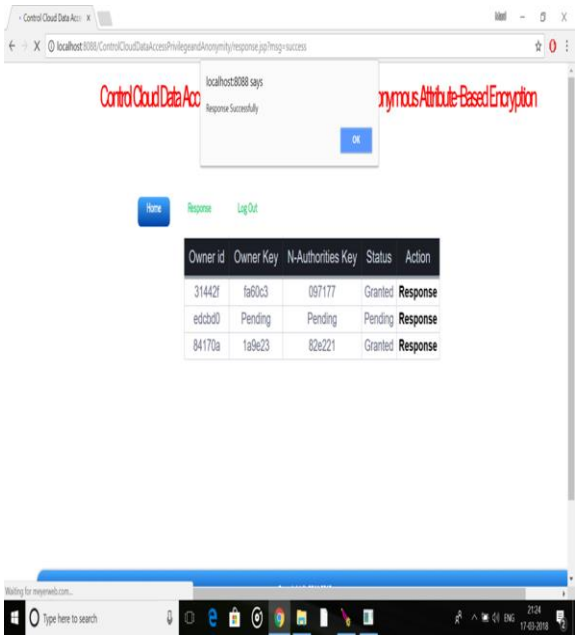



4) Owner Login

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018




5) Request Pending




***Drive HQ***

- Drive HQ creates sub-accounts and assigns different user roles with the group account service.
- Organizes the groups and restricts the privileges given to any file, folder or user.
- With local-to-cloud and cloud-to-cloud backup, you can rest assured your files are secured with drive HQ no matter what happens.

6) Displays the uploaded files


## 6. Conclusion

This paper proposes 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 in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to $N - 2$ authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that Anony- Control both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer.

One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes [39]–[41]

who support efficient user revocation is one of our future works.

## 7. References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.