ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

K.Shravan Naidu
Department of Computer Science and Engineering
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, RR. District, Hyderabad,
Telangana - 501301, India.

J.Rajasekhar
Department of Computer Science and Engineering
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, RR. District, Hyderabad,
Telangana - 501301, India.

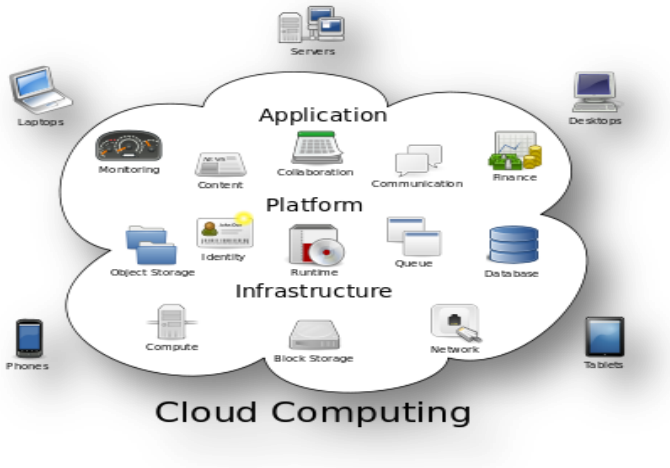
ABSTRACT

We propose a new (without having one central area of command) access control big plan/layout/dishonest plan for secure data storage in clouds that supports unnamed ((checking for truth/proving true) someone's identity). In the proposed big plan/layout/dishonest plan, the cloud (checks for truth/proves true) the realness of the series without knowing the user's identity before storing data. Our big plan/layout/dishonest plan also has the added feature of access control in which only valid users can (change secret codes into readable messages) the stored information. The big plan/layout/dishonest plan prevents replay attacks and supports creation, change, and reading data stored in the cloud. We also address user cancellation. More than that, our ((checking for truth/proving true) someone's identity) and access control big plan/layout/dishonest plan is (without having one central area of command) and strong and healthy, unlike other access control big plans/layouts/dishonest plans designed for clouds which are (controlled by one central place). The communication, computation, and storage overheads are almost the same as (controlled by one central place) approaches.

INTRODUCTION

What is cloud computing?

(computers that do work for you, but that are stored somewhere else and maintained by other companies) is the use of figuring out/calculating useful things/valuable supplies (hardware and software) that are delivered as a service over a network (usually the Internet). The name comes from the common use of a cloud-shaped symbol as a blurry pictures (in your mind) for the complex (basic equipment needed for a business or society to operate) it contains in system diagrams. (computers that do work for you, but that are stored somewhere else and maintained by other companies) trusts remote services with a user's data, software and computation [1-5]. (computers that do work for you, but that are stored somewhere else and maintained by other companies) consists of hardware and software useful things/valuable supplies made available on the Internet as managed third-party services. These services usually provide access to advanced software computer programs and high-end networks of server computers [3].



Structure of cloud computing

Cite this article as: K.Shravan Naidu & J.Rajasekhar, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 4 Issue 11, 2017, Page 440-448.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

How Cloud Computing Works?

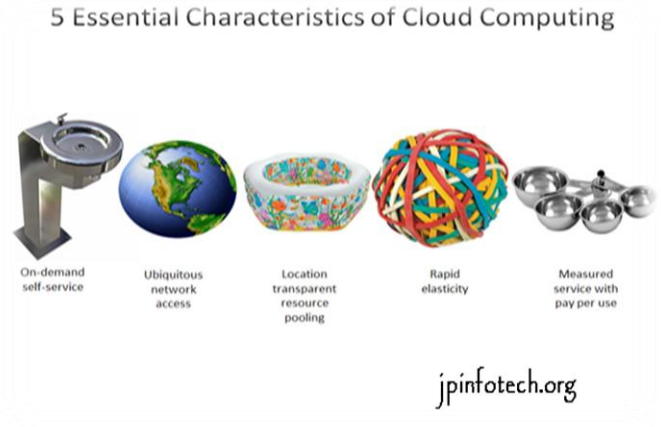
The goal of (computers that do work for you, but that are stored somewhere else and maintained by other companies) is to apply traditional supercomputing, or high-performance figuring out/calculating power, (usually/ in a common and regular way) used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented computer programs such as (related to managing money) (mixes of stocks, bonds, etc./document collections), to deliver decorated (with a personal touch) information, to provide data storage or to power large, very interesting computer games [7].

The (computers that do work for you, but that are stored somewhere else and maintained by other companies) uses networks of large groups of servers usually running low-cost (related to people who use a product or service) PC technology with (made to do one thing very well) connections to spread data-processing hard jobs across them. This shared IT (basic equipment needed for a business or society to operate) contains large pools of systems that are linked together. Often, virtualization ways of doing things are used to (make as big as possible) the power of (computers that do work for you, but that are stored somewhere else and maintained by other companies).

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

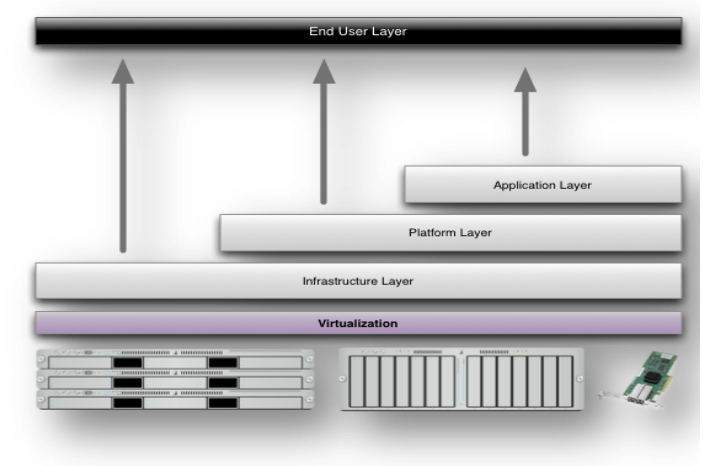


Characteristics of cloud computing

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Services Models:

Cloud Figuring out/calculating contains/makes up three different service models, namely (basic equipment needed for a business or society to operate)-as-a-Service (IaaS), (raised, flat supporting surface)-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [9]. The three service models or layer are completed by an end user layer that combines all the features of the end user opinion about (computer services other companies do for you over the Internet). The model is shown in figure below. If a cloud user accesses services on the (basic equipment needed for a business or society to operate) layer, for instance, she can run her own computer programs on the useful things/valuable supplies of a cloud (basic equipment needed for a business or society to operate) and remain responsible for the support, maintenance, and security of these computer programs herself. If she accesses a service on the application layer, these tasks are (usually/ in a common and regular way) taken care of by the (computer service another company does for you over the Internet) provider [2].



Structure of service models

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

EXISTING SYSTEM:

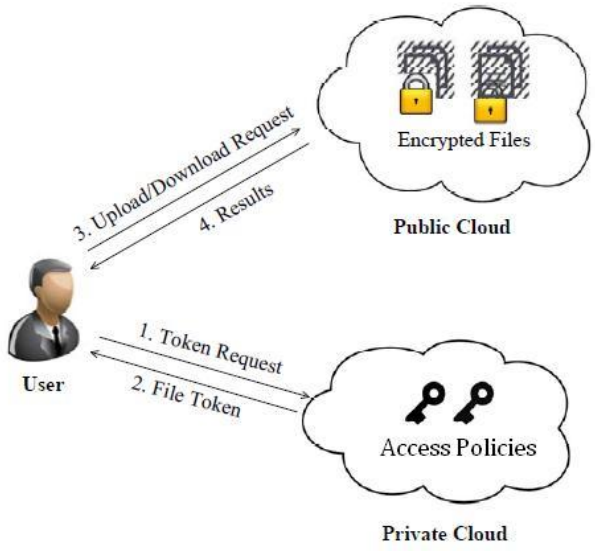
Existing work on access control in cloud are (controlled by one central place) in nature. Except and, all other big plans/layouts/dishonest plans use ABE [4]. The big plan/layout/dishonest plan in uses a (having a left half that's a perfect mirror image of the right half) key approach [6] and does not support (verifying someone's identity). The big plans/layouts/dishonest plans do not support (verifying someone's identity) also.

It provides privacy preserving (identity is verified) access control in cloud. However, the authors take a (controlled by one central place) approach where a single key distribution center (KDC) [8] distributes secret keys and attributes to all users.

DISADVANTAGES OF EXISTING SYSTEM:

- The scheme in uses asymmetric key approach and does not support authentication.
- Difficult to maintain because of the large number of users that are supported in a cloud environment.

SYSTEM ARCHITECTURE:



PROPOSED SYSTEM:

We propose a new (without having one central area of command) access control big plan/layout/dishonest plan for secure data storage in clouds that supports unnamed (verifying someone's identity).

In the proposed big plan/layout/dishonest plan, the cloud (checks for truth/proves true) the realness of the series without knowing the user's identity before storing data.

Our big plan/layout/dishonest plan also has the added feature of access control in which only valid users can (change secret codes into readable messages) the stored information.

The big plan/layout/dishonest plan prevents replay attacks and supports creation, change, and reading data stored in the cloud.

ADVANTAGES OF PROPOSED SYSTEM:

- Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them [10].
- Authentication of users who store and modify their data on the cloud.
- The identity of the user is protected from the cloud during authentication.

IMPLEMENTATION MODULES:

- System Initialization.
- User Registration.
- KDC setup.
- Attribute generation.
- Sign.
- Verify.

MODULES DESCRIPTION:

System Initialization:

Select a prime q, and groups G1 and G2, which are of order q. We define the mapping ˆe : G1 ×G1 → G2. Let g1, g2 be generators of G1 and hj be generators of G2, for j ∈ [tmax], for arbitrary tmax. Let H be a hash function. Let A0 = ha0 0 , where a0 ∈ Z∗ q is chosen at random. (TSig,TV er) mean TSig is the private key with which a message is signed and TV er is the public key

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

used for verification. The secret key for the trustee is TSK = (a0, TSig) and public key is TPK = (G1,G2,H, g1,A0, h0, h1, . . . , htmax, g2, TV er) [11].

User Registration:

For a user with identity Uu the KDC draws at random Kbase ∈ G. Let K0 = K1/a0 base . The following token γ is output γ = (u,Kbase,K0, ρ), where ρ is signature on u||Kbase using the signing key TSig.

KDC setup:

We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs [12] in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.

Attribute generation

The token verification algorithm verifies the signature contained in γ using the signature verification key TV er in TPK. This algorithm [13-15] extracts Kbase from γ using (a, b) from ASK[i] and computes Kx = K1/(a+bx) base , x ∈ J[i, u]. The key Kx can be checked for consistency using algorithm ABS.KeyCheck(TPK,APK[i], γ,Kx), which checks ˆe(Kx,AijBx ij) = ˆe(Kbase, hj), for all x ∈ J[i, u] and j ∈ [tmax].

Sign:

The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.

Verify:

The verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs.

Algorithm

Attribute-Based Encryption

System Initialization

Select a prime q, generator g of G0, groups G0 and GT of order q, a map e : G0 _ G0 ! GT , and a hash function H : f0; 1g_ ! G0 that maps the identities of users to

Encryption by Sender

The encryption function is ABE:EncryptðMSG; XÞ. Sender decides about the access tree X. LSSS matrix R can be derived as described Sender encrypts messag

Decryption by Receiver

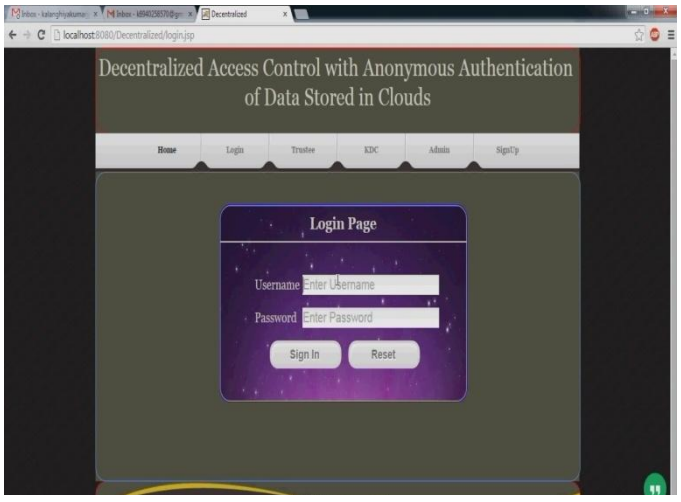
The decryption function is ABE:DecryptðC; fski;ugÞ, where C is given Receiver Uu takes as input ciphertext C, secret keys fski;ug, group G0, and outputs message

Attribute-Based Signature Scheme

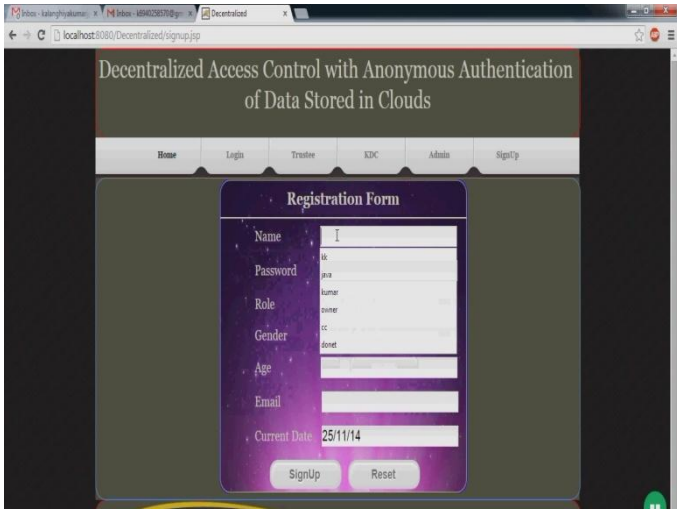
System Initialization

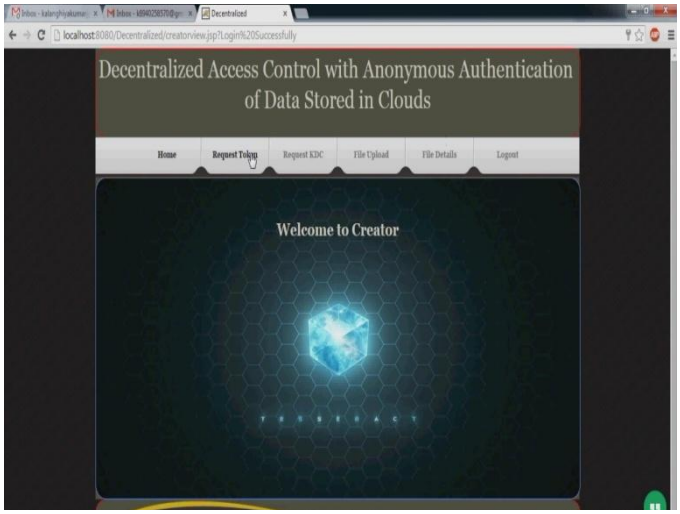
Select a prime q, and groups G1 and G2, which are of order q. We define the mapping ^e : G1 _ G1 ! G2. Let g1; g2 be generators of G1 and hj be generators of G2, for j 2 ½tmax_, for arbitrary tmax. Let H be a hash function. Let A0 ¼ ha0 0 , where a0 2 ZZ_ q is chosen at random

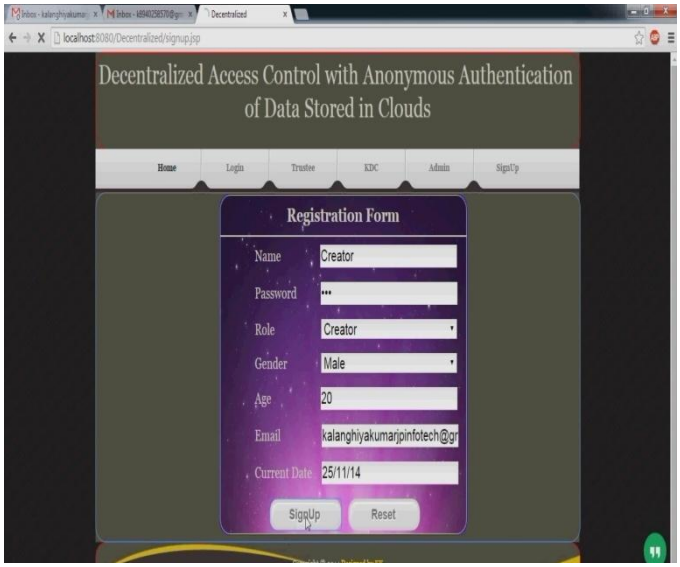
SCREEN SHOTS

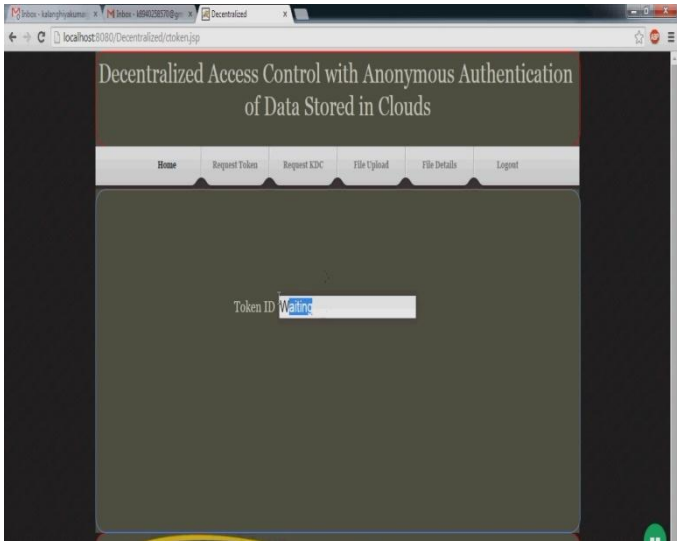


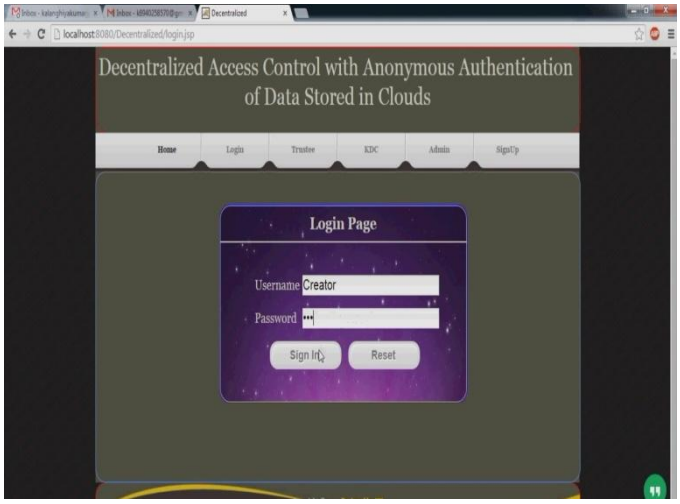
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



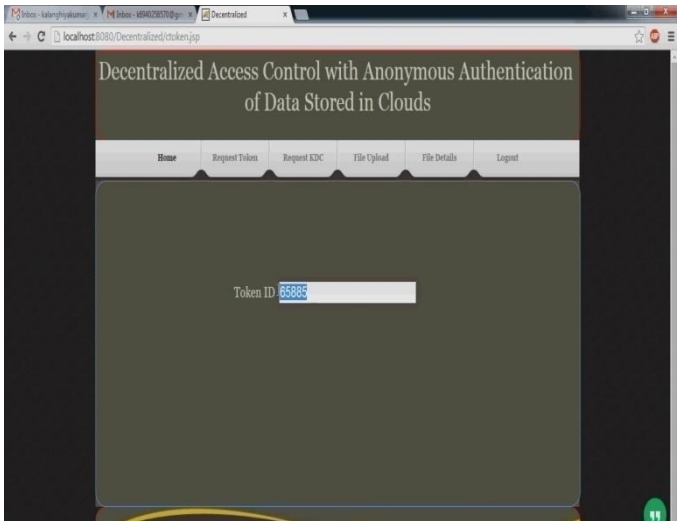


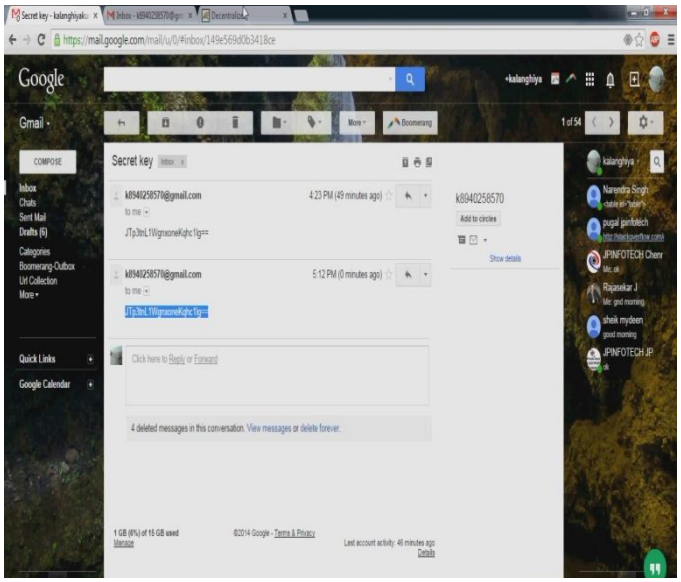


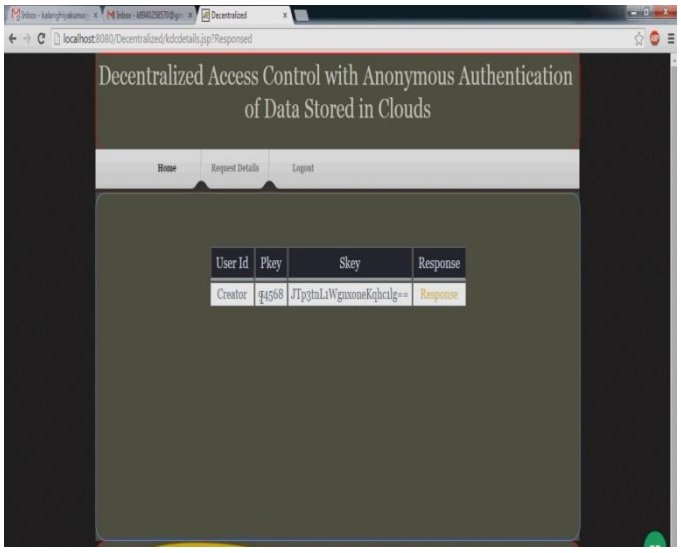


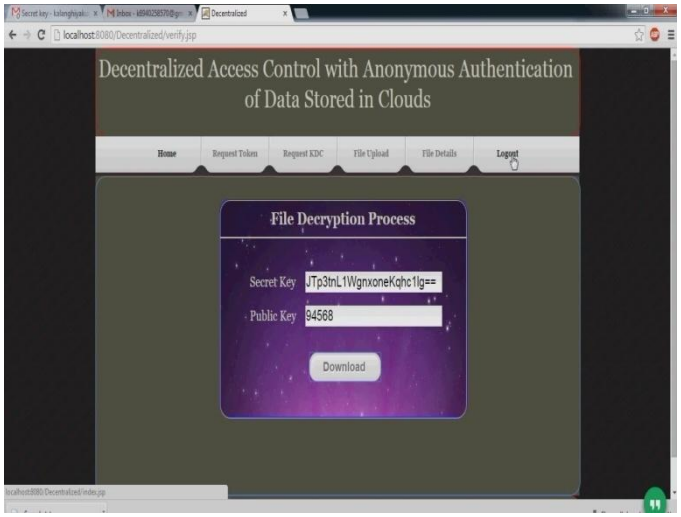


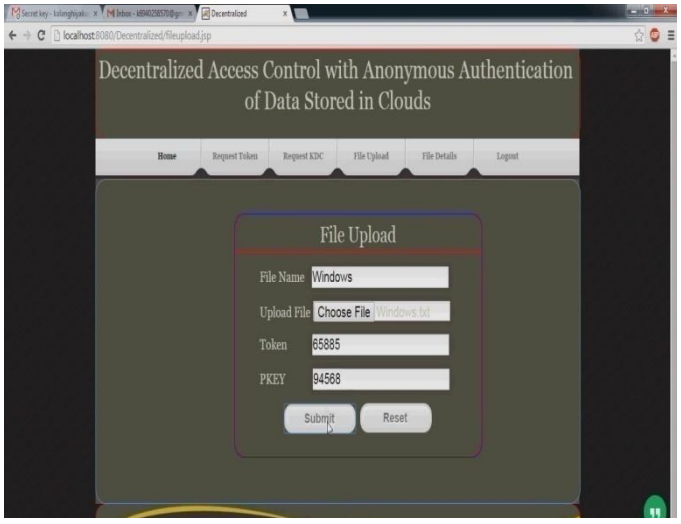
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal











Limitations & Future Enchantements

One limitation is that the cloud knows the access policy for each record stored in the cloud. we would like to hide the attributes and access policy of a user

We have presented a (without having one central area of command) access control way of doing things with unnamed (verifying someone's identity), which provides user cancellation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only (checks for truth/proves true) the user's (written proof of identity, education, etc.). Key

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

distribution is done in a (without having one central area of command) way.

The most expensive operations involving pairings and is done by the cloud. If we compare the computation load of user during read we see that our big plan/layout/dishonest plan has similar costs. Our big plan/layout/dishonest plan also compares well with the other verified big plan/layout/dishonest plan

We present the computation complex difficulty of the privacy preserving access control rules of conduct. We will calculate the computations needed/demanded by users and that by the cloud. Table 2 presents notes/ways of writing used for different operations

CONCLUSION

We have presented a (without having one central area of command) access control way of doing things with unnamed ((checking for truth/proving true) someone's identity), which provides user cancellation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only (checks for truth/proves true) the user's (written proof of identity, education, etc.). Key distribution is done in a (without having one central area of command) way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

REFERENCES

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

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

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

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

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

[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

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

[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

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

[10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

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

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

[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.