A Fine Tuned Data Access using ABE

Vinodkumar.B[1] Sachin S.[2]
[1]Assistant Professor [2]MCA Student
[1,2]Department of Master of Computer Applications
[1,2]Dayananda Sagar College of Engineering, Bangalore-78, India

Abstract— “A Fine Tuned Data Access Using ABE” mainly focuses on securing the access of file data for the authorized personnel within a group or within an organization. Its secured access of data can be achieved through one of the concepts of ABE. Since there is a huge amount of data being transferred within an organization, securing the data is very important to avoid misuse of data by an unauthorized person.

Key words: ABE-Attribute Based Encryption. CP-ABE Cipher-Text ABE

I. Introduction

The first introduction of Attribute Based Encryption (ABE) was in the distributed system. The User when quits the organisation could still access the data using the key he possessed. This needed the control. This issue can be solved in a better way, if the concept of Cipher-Text ABE is adopted to the existing system. The following improvisation has to be made:

A. *Setup*

The cipher-text ABE (CP-ABE) has to be installed and the environment has to be setup on the data owner’s machine for securing the data transfer/sharing. Any security rule will be the input field which has to yield an output key which is public.

II. Literature Survey

A. *Existing and Proposed System*

In the existing system, when a client quits the organization/group he/she is removed from the group list by the supervisor. Removal from the group does not make the user/operator private

Keys inactive. This indicates that he can still be in the group as an active member. The active Members of the group are not aware of the removal of the user/operator as they can still view the user through their private keys. This poses a threat and it is a challenge for security. For better understanding, if the information is encrypted under this attribute “professor AND cryptography” with the key that is public of that group. Consider two of the users that are using this system: A and B where the keys are private are being linked to the set of traits {cryptography, male, professor} and {student, cryptography, male}. If both the members are inside the same group and keep the key that is secret, then the information can be decrypted by A and not by B. If A is removed from the team, then A alone cannot decrypt as he will never have that key which is secret to the group that was updated. But here the traits of A are never removed and B has the key that is secret of this group. Hence, A can do the operation of collusion with B in order to decrypt the information. There was no model of security and that of proof in this system. This condition is called collusion problem which is major challenge.

- It is expensive in communication and computation load for users.
- Performing encryption decryption requires high computation range. This becomes difficult due to limited computer resources.

B. *Proposed System*

Present systems are designed for maximum benefit by operator removal for storing in the cloud, which is a better efficient Cipher-Text ABE.

- With users in cooperation with one another the operation of collusion can be avoided.
- Furthermore, we build an efficient user removal method based on Cipher-Text ABE by making the past scheme better and ensuring better security.
- A certificate is included into every operator’s key which is private for better security. Hence, every group key that is secret is very much distinguished compared to others with some traits embedded with key that is private.
- Encryption Cloud Service Provider(ECSP)and Decryption-Cloud Service Provider(D-CSP) are two servers which help in reducing the period of computation and burden in the user.[1]
- The function of Encryption-CSP and the Decryption-CSP is to perform the operation of encryption and decryption.
- Advantages of the proposed system:
- Less computation burden on the user’s machine
- Cost effective
- Most of the load is in E-CSP and D-CSP hence distributing work.[3]
- It is efficient for resource limited device such as cell phones.
- Utilized in the cloud systems storage requiring this ability of user removal and fine-tuned data access.

III. Feasibility Study

In this current stage the viability of this system is done where such business proposals must be advanced which can be a broader planning and implementation to this system with budget planning. During the course of system study the viability study for the proposing system has to be finished in due course. This guaranteed viable proposition shall not be a burden to the said workforce. In viability examination, general awareness of the fact prerequisites for the framework is the first step.

IV. Operational Feasibility

These studies are for checking levels of total acceptance making the clients use the systems with a better way in ease. The Systems must not make these clients very uncomfortable. Heights of acceptance from clients mainly focusing in the different kinds of methodologies used in teaching the operators and making him/her better with the systems.

V. Functional Requirements

Functional Requirements defining an element of this software system, how the systems must function when a particular data source is given or in any conditions which include counts, information controls and handling and any other particular attributes of usefulness:

A. Cloud

1) Cloud can view all the details of files.
2) Cloud is able to view lists of the downloaded details.

B. Owner

1) Owner can register a new account.
2) With the encrypted key, the owner can upload a file.
3) Owner can view the list once uploaded.

C. Certification Authority

1) The authority account can be activated by Owner.
2) User Id is sent to mail once authentication is done.
3) Being able to see the details.

D. Attribute Authority

1) Can make new registrations.
2) Can perform uploading of files.

E. End User

1) Initiating new user registrations.
2) Viewing details and other information.
3) Viewing content and file downloads using the key that is private to one user.

VI. Non-Functional Requirements

This requirement, as the name says, are those that are not directly worried by the capacities that are very particular with the system. Being identified with emergent properties of the system, such as functionalities like occupancy of store and unwavering. This may also characterize all the constraints of the system, along with the capacity of input and output for the representation of information and all the interfaces. The other being very basic compared to the requirements that are practical. The accompanying non-functional requirements are to be taken care of for a better development of the system.

A. The Key Non-Functional Requirements are:

1) Security

The system should allow secure communication between cloud server & user.

2) Platform Independence

Being able to run on any platform for that matter.

3) Reliability

This system should be reliable enough and should never degrade existing systems performance and must not lead to any lag in the system.

4) Time of Response

Having a quicker time of response.

5) Scalability

Even during dramatic base growth it should provide a good optimal overall performance.

6) Maintainability

Being easy to update and maintain all the services with respect to the system.

B. Fine-Tuned Data Access

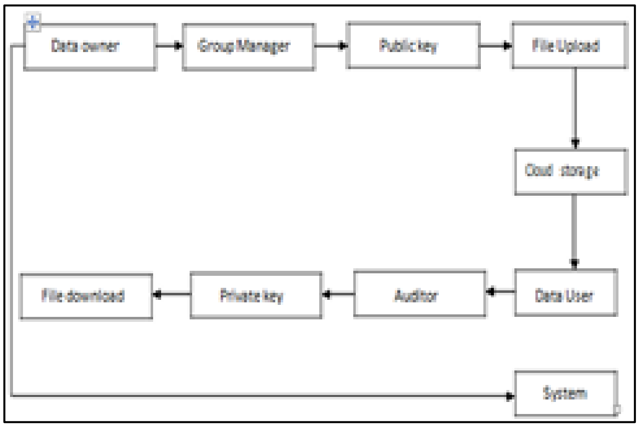

Fig. 1:

System perspective refers to the Diagrams being used which outwardly express the powers following up on the parts of a procedure and the associations between those strengths.

VII. Data Flow Diagrams

A Data Flow Diagram (DFD) is a graphical

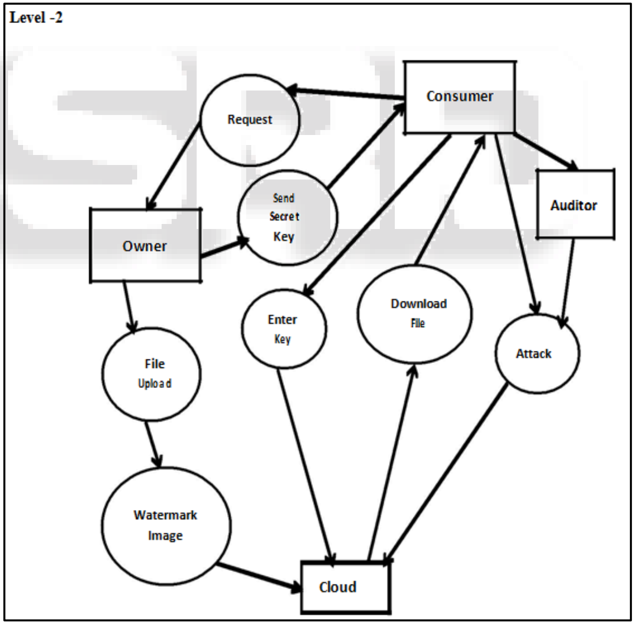

Fig. 2: Level 2 DFD

VIII. Detailed Design

Detailed design is the chart which comprehends the inner stream of control inside the parts of the system. It includes how systems inside segments associates with outside elements like clients of the system. It gives an approach to comprehend the dynamic parts of the system. It helps in breaking down the stream of information and control inside the system and furthermore gives a thought of how the usefulness is invoked by various elements and components inside the system. It gives a general engineering of the system and gives a functional examination and dynamic parts of the system in alternate point of view.

IX. CONCLUSION

The objective of this project was to achieve controlled data access using Cipher-Text-ABE. The aim was to secure the system for remote file accessing. The system had a threat when the existing user left the group or organisation. He could still be an active member and hence could access the data shared in the group. This challenge has been addressed by the current system by using the policy of CP-ABE, which ensures complete data security with controlled access through private key access. Having operator removal in a better way, the CP-ABE has turned out to be an efficient policy for the system. Constructing a strict Cipher-Text-ABE proposal that is totally based on DiffeHelman (DH) belief by, overcoming of the collusion threats, and including a certificate into keys that are private to the operator/user. This helps in a proper security framework where the removed users will be never having an option to compose a proper private key that is valid, in addition to their keys that are private. Applying the concepts of outsourcing the load to servers (Encryption-cloud service provider and Decryption-cloud service provider) helps one to eventually reduce the load of computation and also help the operator to reduce the factor of risk that might possibly occur. Proving efficiency in all domains the framework also proves that it is also very efficient in devices having limited resources.

X. FUTURE ENHANCEMENT

The system 'Fine Tuned Data Access Using ABE' is operational and providing controlled data access of the remote files shared within the group/organization. However, there is a lot of scope for improvement for the system to perform more efficiently.

The following observations have been made to improvise the framework:

Improvised user-interface can be designed for better operation.

- Private Key can be sent over text messages on the mobile phone.
- Data leakage detection mechanism can be implemented.

REFERENCES

[1] J.Bethencourt, A.Sahai and B.Waters, "Ciphertext-Policy Attribute-Based Encryption, "Proc. IEEE Symposium on Security with Privacy, pp.321-334, May2007, doi:10.1109/SP.2007.11

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc.5th ACM Symposium on Information, Computer and Communications Security (ASIACCS' 10), pp. 261-270, 2010.

[3] L. A. Treinish M. L. Gough "A software package for the data independent management of multi-dimensional data" <em>EOS Trans. Am. Geophysical Union</em> vol. 68 no. 28 pp. 633-635 Jul. 1987.

[4] Calvanese D. Lenzerini M. and Nardi D. 1998. Description logics for conceptual data modeling. In Logics for Databases and information Systems J. Chomicki and G. Saake Eds. Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers Norwell MA 229-263.