International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Identity Based Data Sharing Security in Cloud Computing

Arunkumar[1], Dr.S.M.Joshi[2]

[1]*Student, Dept. of Computer Science & Engineering, Shri Dharmasthala Manjunatheshwara College of Engineering, Dharwad, Karnataka, India*

[2]*Professor, Dept. of Computer Science & Engineering, Shri Dharmasthala Manjunatheshwara College of Engineering, Dharwad, Karnataka, India*

Abstract - *Evolution of Cloud computing provides a versatile and convenient method for information sharing that brings numerous edges for each the society and people. Thus, it's important to put cryptographically increased entrance management on the shared statement. Identity-based encoding could be a hopeful cryptological primitive to make sensible information sharing system. Consequently, it'll provides a secure information sharing between approved customers, and so, it'll avoid information breach, data loss and provides secure information to the desired customers.*

Key Words: Cloud Computing, TPA, PKI,IDE(Identity Based Encryption), CSP.

1. INTRODUCTION

Many trends square measure gap up the age of Cloud Computing, which is Associate in Nursing Internet-based development and use of technology. Cloud computing is the dealing of computing as a service rather than a resource, whereby shared resources, software, and instruction square measure provided to computers and alternative devices as serviceability over a network.

Cloud computing furnishes computation, software, information access, and storage services that do not need end-user information on the physical location and configuration of the system that recommends the services. Parallels to this conception square measure usually drawn with the electricity grid, whereby end-users consume power while not having to understand the part devices or infrastructure needed to provide the service.

Cloud computing describes a replacement supplement, consumption, and delivery model for IT services supported web protocols, and it generally involves provisioning of dynamically climbable and generally virtualized resources. It's a byproduct and outcome of the ease-of-access to far-out computing sites provided by the network.

This might take the form of web-based tools or applications that users will access and use through a web browser as if the programs were put in domestically on their computers.

In this paper, we tend to address this open issue and propose a secure and climbable fine-grained information access management theme for cloud computing. Our projected theme is partly supported by our observation that, in application situations, every file square measure usually associated with a bunch of attributes that square measure meaningful within the context of interest. The access structure of each user will, therefore, be outlined as a singular logical expression over these attributes to replicate the scope of data files that the user is allowed to access the data.

2. Literature Survey

In this paper [1][2], IBE eliminates the need for providing a public key infrastructure (PKI). Irrespective of the setting of IBE or PKI, there must be an approach to blackout users from the system when essential, e.g., the authority of some user is expired or the confidential key of some utilizer is disclosed. In the traditional PKI setting, the problem of revocation has been well studied, and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates.

This paper discusses the conception of Cloud Computing to comprehend a complete definition of what a Cloud is, victimization the foremost characteristics generally associated with this orientation at intervals the literature. Over twenty definitions square measure studied permitting the extraction of an agreed definition conjointly as a minimum definition containing the essential characteristics. This paper says abundant attention to the Grid paradigm because it is usually confused with Cloud technologies. We tend to conjointly describe the relationships, and distinctions between the Grids and Cloud approaches [3].

This paper [4] Using Cloud Storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, outside the discharge of local data storage and maintenance. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the safeness of outsourced data and be worry-free.

In this paper[5] new orientation of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in

the cloud. Some existing remote orientation checking methods can only serve static exhibit data and thus cannot be applied to the auditing service since the data in the cloud can be apathetically updated. Thus, a dashing and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud.

3. Proposed Method

In this paper, 1st we tend to log in to google cloud services, and so, we tend to produce our instances, and so, we tend to introduce a notion known as rescinding able storage identity-based encoding for building a cheap information sharing system that fulfills the 3 security goals. A lot of exactly, the subsequent achievements square measure captured in this paper. We offer formal definitions for IBE and It's corresponding security model we tend to gift a concrete construction of IBE. The projected theme will offer confidentiality and backward/forward two secrecy at the same time. the proposed scheme can withstand decryption key exposure, The proposed scheme is efficient when it procedure of ciphertext update only needs public information.

In the cloud environment, three members are very important. They are Data Owner, Cloud Service Provider (CSP), Data User. These three members securely share the data. For that, the data owner must create access control in the cloud service provider. Then only the data owner can upload the data and the user can retrieve the data.

3.1 Information confidentiality

Unauthorized users ought to be prevented from accessing the plain text of the shared information hold on within the cloud server. Additionally, the cloud server, that is supposed honestly however curious, ought to even be deterred from knowing plain text of the shared information.

3.2 Backward secrecy

Backward secrecy implies that once a user's authorization is terminated, or a user's secret key's compromised, he/she ought to be prevented from accessing the plain text of the after shared information that square measure was still encrypted underneath his/her identity.

3.3 Forward secrecy

Forward secrecy implies that once a user's authority is terminated, or a user's secret key's compromised, he/she ought to be prevented from accessing the plain text of the shared information which will be antecedently accessed by him/her.

3.4 IBE

We propose a completely practical identity-based encoding theme (IBE). The theme has chosen cipher text security at intervals the random oracle model assumptive a variant of the machine Diffie-Hellman drawback. Our system is based on additive maps between teams. The Well pairing on elliptic curves is Associate in Nursing example of such a map. We tend to provide precise definitions for secure identity primarily based encoding schemes and provides many applications for such systems.

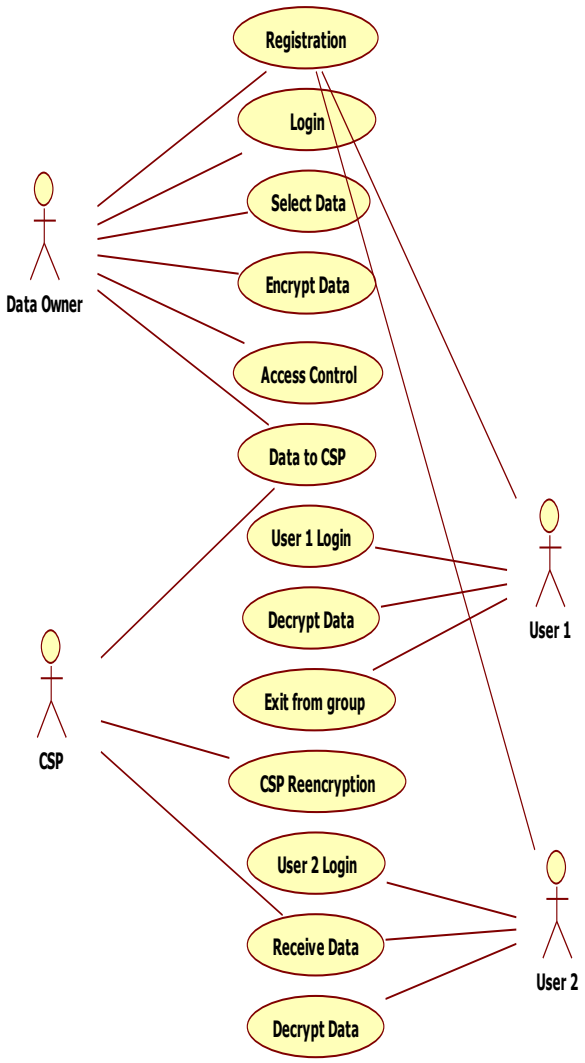

Fig 1 Use Case Diagram

4. Experimental Results

In cloud computing, consumers host their information on cloud servers and, users (data consumers) will access the data from cloud servers. The analysis and simulation results show that our projected auditing protocols square measure secure and economical, particularly it cut back the computation the price of the auditor.

This result will give a logic to use of the new system such as the screen flow, screen design, type of help on the

screen, type of errors while outward the data, the corresponding validation check at each entry, and the ways to correct the data entered. This coaching may be different across different user groups and different levels of hierarchy.

The user of the system must be is made hardbitten and comfortable with the environment. documentation furnishing the whole operations of the system is being developed. Useful solutions and guidance are given inside the application itself to the user. The system is developed user-friendly so that the user can work the system from the solutions given in the application itself.

OUTCOMES:

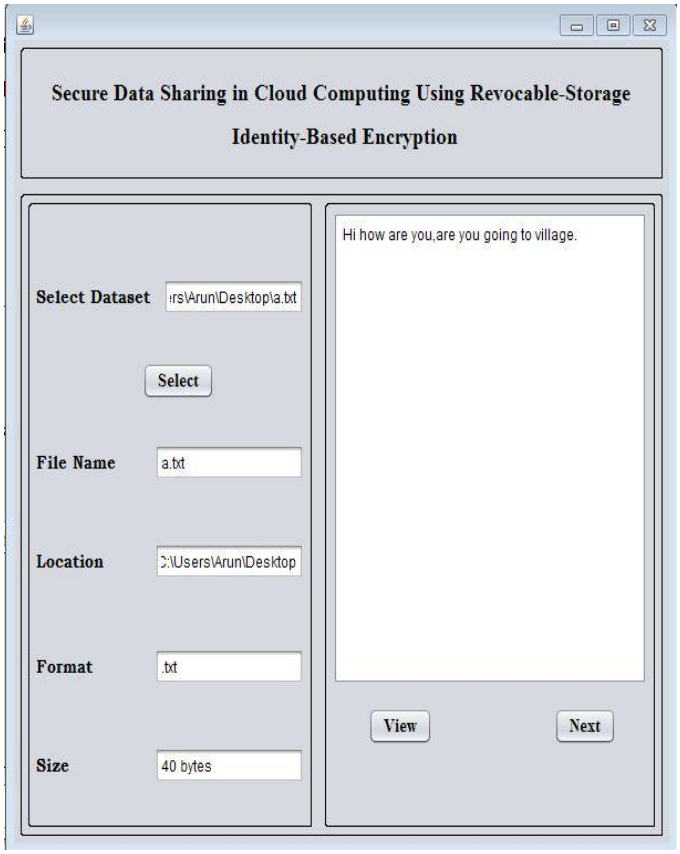

Fig 2 Information of data

Fig 3 Single Encryption using PKI

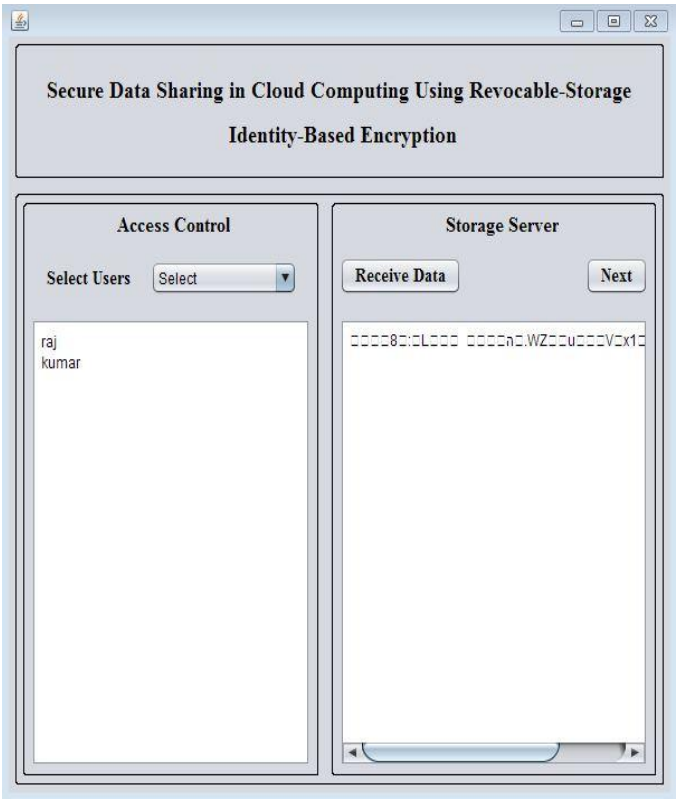

Fig 4 IBE through authorized users

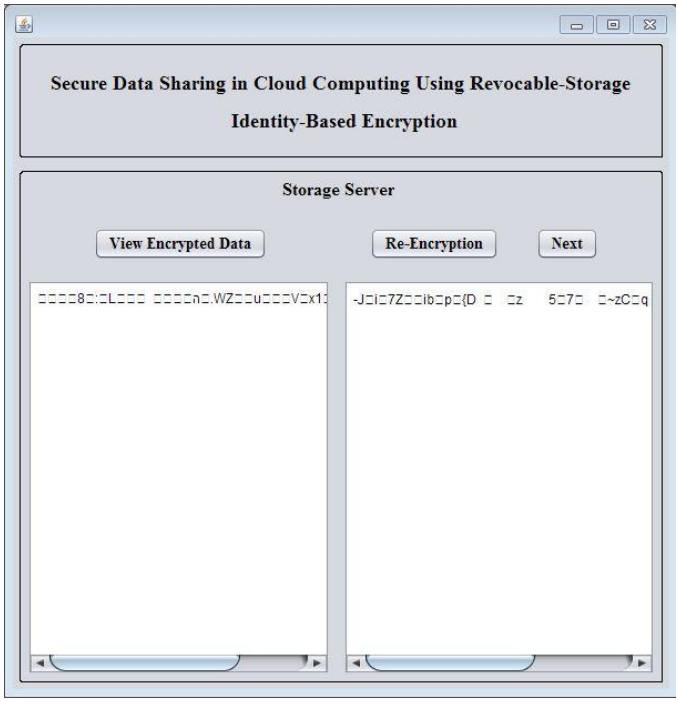

Fig 5 Double Encryption using PKI

5. CONCLUSION

In this paper, Cloud computing brings nice convenience for individuals. Significantly, it matches the increase would like of sharing information over the net. In this paper, to operate a cheap and secure information sharing system in cloud computing, we tend to project a notion known as IBE, that supports identity revocation and ciphertext update at the same time specified revoked user is prevented from accessing antecedent shared information, yet as after sharing information.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Public auditing for shared information with economical user revocation at intervals the cloud," in INFO COM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[2] Jianghong Wei dynasty, Wen Fen Li, Xuexian HU, " Secure information Sharing in Cloud Computing victimization Revocable-Storage Identity-Based Encryption", 2015, IEEE Gregorian calendar month 2015.

[3] K. Yang and X. Jia, "An economical and secure dynamic auditing protocol for information storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726,2013.

[4] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage Computers", IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[5] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds Parallel and Distributed Systems", IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[6] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing Services Computing", IEEE Transactions on, vol. 5, no. 4, pp. 551–563,2012.