International Journal for Modern Trends in Science and Technology, 8(09): 52-56, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809008
Available online at: http://www.ijmtst.com/vol8issue09.html

Incurring of Cloud Data with Attribute Based Access Control in Decentralized Clouds

GeethaBhavani P | Antharaju K Chakravarthy

Aditya Engineering College, Surampalem, India.
Jawaharlal Nehru Technological University Kakinada, EG District, AP, India

To Cite this Article
GeethaBhavani P and Antharaju K Chakravarthy. Incurring of Cloud Data with Attribute Based Access Control in Decentralized Clouds. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 52-56. https://doi.org/10.46501/IJMTST0809008

Article Info
Received: 16 July 2022; Accepted: 20 August 2022; Published: 06 September 2022.

ABSTRACT

Data hosted on untrusted sites like clouds need fine grained access control. A decentralized approach to key management is recommended over a centralized one due to the sheer amount of data involved. Encryption and decryption may be costly and impractical when data is accessed from devices with limited resources. Using rapid encryption, outsourced decryption, and user revocation, we devise an ABE decentralized system. Our method is tailored to the mobile cloud environment because it relies on the cloud to store encrypted data and partially decipher cipher texts, and because users with mobile devices may upload data to the cloud or get data from it for very low cost in encryption and decryption, respectively. Pre-processing is done offline and encryption is done online in a two-step process: an offline phase that occurs while the device is inactive, and an online phase that occurs when the policy is applied. This is quicker and more efficient than current decentralized ABE systems.. It is necessary for data consumers to develop a modified version of the decryption key in order to enable an untrusted proxy server to partly decode the cipher text without having access to the plaintext.. Once the cipher text has been partly decrypted, users will not have to execute any expensive pairing procedures to finish decrypting it. We also include user revocation in this system without paying extra costs online. Compared to existing ABE schemes, ours greatly decreases calculation times for both data owners and data consumers and is particularly appropriate for application in mobile devices.

Keywords: Encryption, Cloud computing, Servers, Performance evaluation, Access control

1. INTRODUCTION

Consider a typical situation in which data owners desire to transfer their data to untrusted servers like the cloud for long-term storage. In spite of their small storage capacities, cell phones, wireless sensors, and smartcards are all capable of storing large amounts of data. The goal is to preserve the data as long as possible while making it accessible to as many individuals as feasible. Because of the apparently limitless storage capacity that CSPs provide, individuals and organisations are increasingly turning to them for their data storage needs. Many data owners don't trust cloud service providers (CSPs) because of their reputation for being wicked. All data in the cloud has to be protected as a result of this requirement. To ensure that only people with the right credentials may see their data, data owners can set up access controls. Institutions may one day upload to the cloud data from clinical trials evaluating the effectiveness of new drugs on cancer patients. Access to this extremely sensitive information is restricted to medical professionals and researchers involved in the creation of new medications. In this case, attribute-based encryption (ABE) [13] may be used to encrypt data. Decentralised or multi-authority ABE systems are very beneficial in practice since they do not rely on a single authority to generate and distribute decryption keys connected to various qualities.. In certain cases, a patient's medical records may be sent to a medical researcher by a research organisation, rather than the hospital. Because of changes in the work environment, location, etc., user characteristics are always evolving.. Someone who was previously authorised access to data may no longer be eligible. If the user's characteristics have changed, they may still access data. Thus, cancellation of users is important for ABEs. Further complicating matters is the adoption of such powerful encryption methods. Creating revocation keys or decryption can't be done quickly enough on a machine with limited resources. Decentralized attribute-based encryption (ABE) with quick encryption, outsourced decryption, and user revocation is the solution to this problem.. The mobile cloud's storage demands and partial decryption are tailored to our technology, allowing DropBox customers with mobile devices to upload and access encrypted data from DropBox without paying huge expenses for encryption and decryption, respectively. It's possible for the encryption to take longer than expected, the device is charging, or it's inactive, therefore the most costly operations are performed offline as a solution to the issue of encryption being too expensive. During the online phase, just a few calculations are performed, allowing users to continue working without any interference from the gadget.

As a result, data owners may avoid the time and effort of executing decryption procedures on their own. An altered decryption key allows for partial decoding of encrypted data by the proxy server. Partial decryption, on the other hand, is useless to a rogue proxy server. With a few easy procedures, the final plaintext may be decoded from the cipher text. Similar to revocation keys, they may be produced offline and then sent to the proxy server after a few calculations for key transformations are performed online. We'll build the groundwork for our approach by examining these two case studies.

Wi-Fi-enabled sensor networks are becoming more popular as a means of gathering data on the physical, physiological, and behavioral characteristics of the ageing population. Encryption is required to keep this data safe for future use. Academics and caregivers alike may profit from this knowledge, which can be utilized for early diagnosis and intervention, as well as environmental factors, diseases, and the ageing process. Researchers may need to get the necessary criteria from organisations outside of hospitals in order to access data. Individuals from various companies with access to the same data may work together in a collaborative manner. Drop box and similar services enable team members to submit work from their mobile devices while on the road. Encryption must be performed before uploading sensitive data to ensure its protection (financial data, trade secrets etc.). Everyone in the project has access to this data. An organization's members may, however, have their engagement in a project indicated on their resumes in a variety of different ways.

2. LITERATURE REVIEW:

It's becoming increasingly usual to think about cloud access control since it's vital that only authorised users have access to services. Countless terabytes of data, much of it sensitive, are being stored on the cloud. In the cloud, data is encrypted using Attribute-Based Encryption (ABE), which provides several ways to decrypt and decrypt. Customers are given a list of attributes and associated keys in order to aid them in their purchase decisions. Decryption may only be performed by customers that have similar characteristics to those who store data in the cloud [9] [10] Medical therapy may be restricted in many ways, as I discovered while doing my study on the subject. The work of [11] enables cloud-based authenticated access control that safeguards privacy. To this day, researchers still prefer to send secret keys and characteristics to all clients from a single key distribution centre (KDC). In nature, there are too many KDCs to keep track of, making it challenging to manage just one [25]. The game plan When using [12], symmetric key authentication is not supported. No trusted authority was required in [13] to verify that each customer had features from all KDCs, since the multi-authority ABE idea was the focus of the study. Centralized access control is the present state of affairs in the Cloud. As far as attribute-based encryption is concerned, just these two methods exist (ABE). Symmetric key methods used in this methodology do not give authentication. None of the methods provided here can be used for authentication. Work by Zhao et al. enables privacy-preserving authentication for cloud access. KDCs are key distribution centers (KDCs) that provide secret keys and other characteristics to all users. Because of the huge number of users given by the cloud environment[25], maintaining a single KDC might be problematic. As a consequence, we emphasize the need of decentralising the distribution of secret keys and user attributes in the cloud. When it comes to cloud computing, there are several KDCs distributed over the world. ABE is the brainchild of Sahai and Waters [17]. In attribute-based encryption, a user's unique ID is merely one of several qualities that make up a user. There are two types of ABEs. Goyal et al. [18] refers to this as "key-policy ABE," or "KP-ABE." The sender has the ability to encrypt data due to access restrictions in place. It is difficult for a writer whose credentials and set of keys have been removed from the system to re-enter the data. The receiver must know the recipient's characteristics and secret keys in order to decipher encrypted information. When it comes to cipher ext-policy, the receiver implements an AND, OR, and CP-ABE access policy in the form of a tree with attributes as leaves ([19, 20]). A single point of failure is inherent in the KDC because of its centralized approach. Some of the KDCs, according to Chase [21], provide users with characteristics and secret keys. [Anonymous user authentication is made possible by Maji et alABSs 's [22]. As a result, a degree of centralization was sought. Although Maji et al. [23] have provided a decentralized approach; their method does not divulge the names of the users. Re-attempts are a common occurrence while attacking it.

3. PROPOSED SYSTEM:

For decentralized access control, we suggest a CPABE system with rapid encryption and decryption outsourced to a third-party. For the first time, in a decentralized system, a method like ours considerably cuts computing costs for both data owners and data consumers. Because of its decentralization, online/offline mode of encryption, and outsourced decryption capabilities, the CPABE scheme is well-suited for use in real-world scenarios. Decentralized CPABE, introduced by Lewko and Waters [29], serves as our framework. What we've accomplished so far:

1) Fast Online/Offline Encryption: An exponentiation is all that is needed in the online phase of encryption for the most expensive calculations.

2) Outsourced Decryption: The data user may provide encrypted secret keys to the proxy server, which the proxy server can employ to partially decode the data. As a consequence, the data user is only required to execute a fixed amount of exponentiations and no bilinear pairings during complete decryption. Because there is no central authority to decode the data, our system is completely independent of any central authority.

3) Security and performance: Under the assumption that the Lewko-Waters scheme for prime order groups is safe, we establish that our system is secure by replacing the proof sketch with mathematical proofs. This is shown by designing and demonstrating the security of an online offline multi-authority CPABE scheme without outsourced decryption (which was lacking in the previous version).

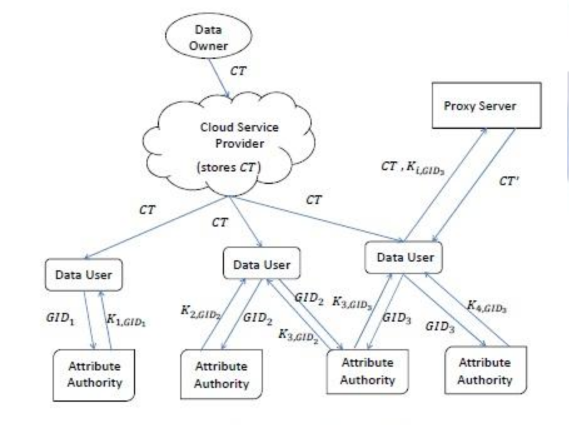
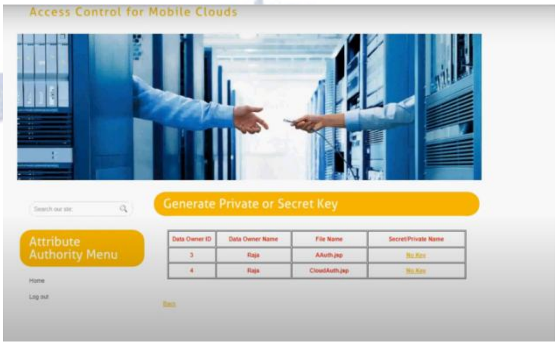


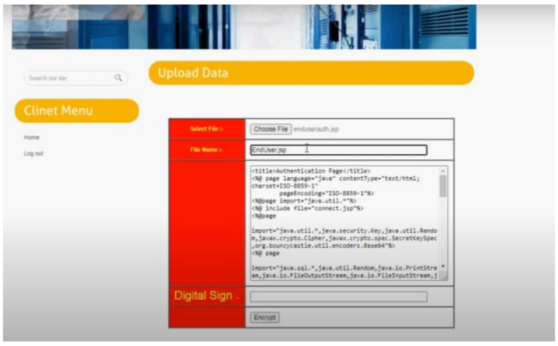
Fig1: System Architecture

4. EXPERIMENTAL RESULTS:


Access Control for Mobile Clouds

Generate Private or Secret Key

Data Owner ID	Data Owner Name	File Name	Secret/Private Name
3	Raja	AAuth.jsp	No Key
4	Raja	CloudAuth.jsp	No Key



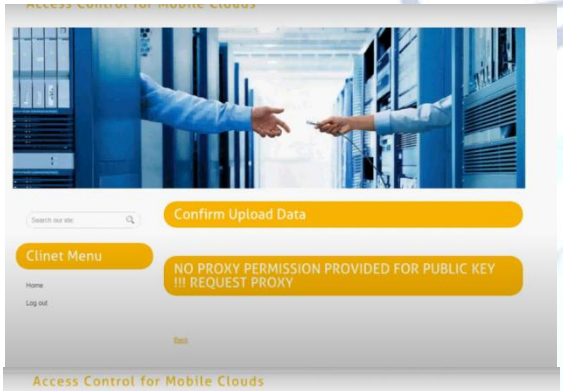
Select File :- Choose File enduserauth.jsp

File Name :- EndUser.jsp

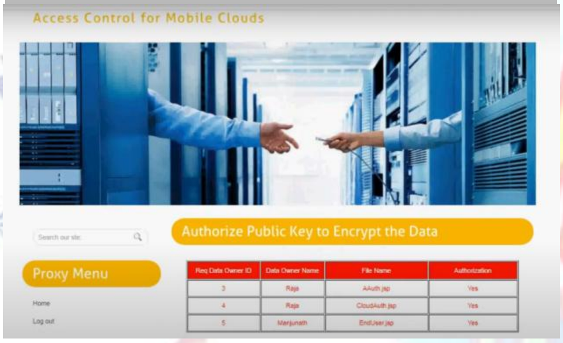
```
<title>Authentication Page</title>
<%@ page language="java" contentType="text/html;
charset=ISO-8859-1"
        pageEncoding="ISO-8859-1"%>
<%@page import="java.util.*"%>
<%@ include file="connect.jsp"%>
<%@page

import="java.util.*,java.security.Key,java.util.Rando
m,javax.crypto.Cipher,javax.crypto.spec.SecretKeySpec
,org.bouncycastle.util.encoders.Base64"%>
<%@ page

import="java.sql.*,java.util.Random,java.io.PrintStre
am,java.io.FileOutputStream,java.io.FileInputStream,j
```

Digital Sign :-

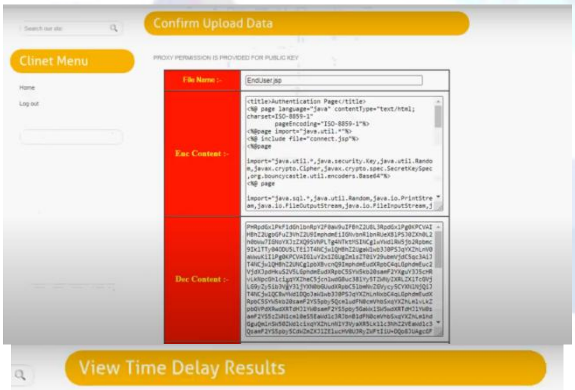
Encrypt



NO PROXY PERMISSION PROVIDED FOR PUBLIC KEY !!! REQUEST PROXY


Access Control for Mobile Clouds
Search our site
Authorize Public Key to Encrypt the Data
Proxy Menu
Home
Log out

Req Data Owner ID	Data Owner Name	File Name	Authorization
3	Raja	AAuth.jsp	Yes
4	Raja	CloudAuth.jsp	Yes
5	Manjunath	EndUser.jsp	Yes



PROXY PERMISSION IS PROVIDED FOR PUBLIC KEY

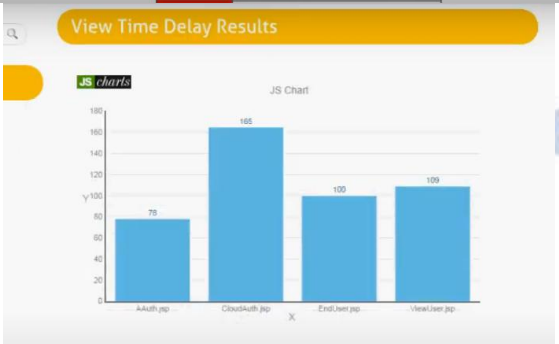
File Name :- EndUser.jsp

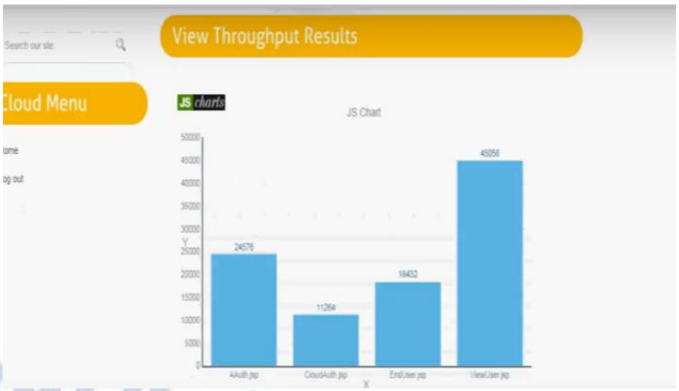
Enc Content :-

```
<title>Authentication Page</title>
<%@ page language="java" contentType="text/html;
charset=ISO-8859-1"
        pageEncoding="ISO-8859-1"%>
<%@page import="java.util.*"%>
<%@ include file="connect.jsp"%>
<%@page

import="java.util.*,java.security.Key,java.util.Rando
m,javax.crypto.Cipher,javax.crypto.spec.SecretKeySpec
,org.bouncycastle.util.encoders.Base64"%>
<%@ page

import="java.sql.*,java.util.Random,java.io.PrintStre
am,java.io.FileOutputStream,java.io.FileInputStream,j
```

Dec Content :-

PHRpdGxlPkF1dGhlbnRpY2F0aW9uIFBhZ2U8L3RpdGxlPg0KPCVAI
HBhZ2UgbGFuZ3VhZ2U9ImphdmEiIGNvbnRlbnRUeXBlPSJ0ZXh0L2
h0bWw7IGNoYXJzZXQ9SVNPLTg4NTktMSINCglwYWdlRW5jb2Rpbmc
9IklTTy04ODU5LTEiJT4NCjwlQHBhZ2UgaW1wb3J0PSJqYXZhLnV0
aWwuKiIlPg0KPCVAIGluY2x1ZGUgZmlsZT0iY29ubmVjdC5qc3AiJ
T4NCjwlQHBhZ2UNCglpbXBvcnQ9ImphdmEudXRpbC4qLGphdmEuc2
VjdXJpdHkuS2V5LGphdmEudXRpbC5SYW5kb20samF2YXguY3J5cHR
vLkNpcGhlcixqYXZheC5jcnlwdG8uc3BlYy5TZWNyZXRLZXlTcGVj
LG9yZy5ib3VuY3ljYXN0bGUudXRpbC5lbmNvZGVycy5CYXNlNjQiJ
T4NCjwlQCBwYWdlDQoJaW1wb3J0PSJqYXZhLnNxbC4qLGphdmEudX
RpbC5SYW5kb20samF2YS5pby5QcmludFN0cmVhbSxqYXZhLmlvLkZ
pbGVPdXRwdXRTdHJlYW0samF2YS5pby5GaWxlSW5wdXRTdHJlYW0s
amF2YS5zZWN1cml0eS5EaWdlc3RJbnB1dFN0cmVhbSxqYXZhLm1nd
GguQmlnSW50ZWdlcixqYXZhLnNlY3VyaXR5Lk1lc3NhZ2VEaWdlc3
QsamF2YS5pby5CdWZmZXJlZElucHV0U3RyZWFtIiU+DQo8JUAgc0F





5. COMPARATIVE STUDY

Table1: Comparative Study

Scheme	Access Control Yes=Y, No=N	Decentralized / Centralized	Read/ Write	Type of Access control	Authentication	Client Revocation
[12]	Y	Centralized	1-W-M-R	Symmetric Key Cryptography	No Authentication	No
[9]	Y	Centralized	1-W-M-R	ABE	No Authentication	No
[15]	Y	Decentralized	1-W-M-R	ABE	No Authentication	Yes
[14]	Y	Decentralized	1-W-M-R	ABE	Not Privacy Preserving	Yes
[11]	Y	Centralized	M-W-M-R	ABE	Authentication	No
[1]	Y	Decentralized	M-W-M-R	ABE	Authentication	Yes
Our scheme	Y	Decentralized	M-W-M-R	KDC (Access Policy), sABE	Authentication	Yes

6. CONCLUSION:

We construct a CPABE scheme in prime order. As stated by the proof of the strategy utilizing random oracles. Prime order groups are used because they are efficient and allow for speedier group operations. Our methodology may be utilized to develop an inefficient Composite order group scheme that relies on higher security principles in the dual system encryption model. It's a future task. This document may address the following issues: Multi-authority online-offline CPABE outsourcing encryption Multi-authority online/offline CPABE The user has no way of knowing whether the partial decryption was successful. Verifiable outsourcing was offered as a solution in our problem's verified outsourcing can be solved similarly. Ours is an honest-but-curious model, therefore we don't discuss it. Changing this assumption requires researching verified decryption outsourcing. We leave it unsolved. This study proposes an ABE for mobile clouds. It has decentralization, rapid encryption, outsourced decryption, and user revocation. All encryption hard calculations are done offline, making the encryption process quicker and more efficient than previous decentralized ABE systems. Untrusted proxy servers partly decode the cipher text without obtaining access to the plaintext, however. Without completing expensive pairing processes, data consumers may entirely unblock partly unlocked encrypted text. Our system allows for online user cancellation without extra fees. Unlike previous schemes, ours achieves a fair combination of encryption and decryption performance while also facilitating decentralization and user revocation.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, "Decentralized Access Control with AnonymousAuthentication of Data Stored in Clouds" IEEE,2014.

[2] Ajith Singh. N, Department of computer science, Karpagam University, Coimbatore, India, M. Hemalatha, Department of software systems & research, Karpagam University, Coimbatore, India, "Cloud computing for Academic Environment".

[3] Luit Infotech Private Limited, Bangalore, India, "Luit Infotech SaaS Business Software".

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

[5] C. Gentry, "A fully homomorphic encryption scheme", Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[6] Yang Tang, Patrick P.C. Lee, John C.S. Lu and Radia Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Transactions on dependable and secure computing, VOL.9, NO. 6, NOVEMBER/DECEMBER 2012

[7] R. Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007

[8] Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Li,"A Secure Cloud Backup System with Assured Deletion and Version Control," Proc. Third Int'l Workshop Security in Cloud Computing, 2011

[9] Personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings," in SecureComm, pp. 89–106, 2010.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.

[11] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, sir. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.

[12] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop (CCSW), 2009.

[13] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.

[14] Ken Yang, Xiaohua Jia and Kui Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", IACR Cryptology ePrint Archive, 419, 2012.

[15] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

[16] Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[19] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.

[20] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[21] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[22] A.B. Lewko and B. Waters, "Decentralizing Attribute Based Encryption,"Proc. Ann. Int' lConf. Advances in Cryptology (EURO- CRYPT), pp. 568- 588,2011.

[23] 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.

[24] "DECENTRALIZED ACCESS CONTROL TO SECURE DATA STORAGE ON CLOUDS"Ankita N.Madde , Minal J. Joshi, Suchita Gutte, Sonal Asawa, Prashant Jawalkar Computer Dept., JSPM's BSIOTR, Pune, India.