CONTROL CLOUD DATA ACCESS PRIVILEGE USING ATTRIBUTE BASED ENCRYPTION

CH Gowthami
Dept of IT, MLRIT,
Hyderabad, India.

G G. Sreeja
Dept of IT, MLRIT,
Hyderabad, India.

B. Rajitha
IT, MLRIT, India

Abstract— ***Cloud computing is a radically new computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources , but the data is deployed to some cloud servers, and various privacy concerns emerge from it. Various layouts based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work targets on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, a semi-anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in current access control schemes. AnonyControl decentralizes the central authority to limit the identity origin and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, which privileges of all operations on the cloud data can be managed in a compact structured manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security presentation shows that both AnonyControl and AnonyControl-F are secure under the Diffie Hellman assumption, and our performance estimation exhibits the feasibility of our schemes.***

Keywords- **Cloud computing, Anonycontrol, Access control, Privilege control, Semi anonymity, fully anonymity.**

I. INTRODUCTION

Cloud computing is a complete computing technique, by which computing resources are provided dynamically via Internet and the data storage is outsourced to someone or some party in a ‘cloud’. It greatly attracts attention an-d interest from both academia and industry due to the profit-making, but it also has at least three challenges that must be handled before coming to our reality to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data seclusion is not only about the data contents. Since the most attractive part of the cloud computing is the outsourcing of computation, it is far beyond enough to just oversee an access control. More likely, users want to control the right of data manipulation over other users or cloud servers. [1] [2] This is because when sensitive information or computation is outsourced to the cloud servers or user, which is out of users’ control in most cases, privacy risks would raise constantly because the servers might illegally inspect users’ data and access sensitive information, or other users might be able to infer careful information from the outsourced computation. Therefore, not only the access but also the operation should be managed. Secondly, personal information (defined by each user’s attributes set) is at risk because user's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As everyone is becoming more concerned about their identity privacy these days, the identity privacy also has to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client’s personal data. Last but not least, the cloud computing system should be resilient in the case of security breach in which half part of the system is compromised by attackers. [1]

II. LITERATURE SURVEY

1. Cipher text-Policy Attribute-Based Encryption

AUTHORS: Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan

In several distributed systems a user can able to access data if a user posses a certain set of credentials or attributes. Presently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server stores the data, which is compromised, then the confidentiality of the data will be compromised. In this paper, we present a process for realizing complex access control on encrypted data that we say Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; [2] moreover, our systems are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to explain the encrypted data and built policies into user's keys; while in our system attributes are used to explain a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our systems are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we ensure an implementation of our system and give performance measurements. [1]

2. Multi-authority attribute based encryption with honest-but-curious central authority

AUTHORS: Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi

An attribute based encryption scheme capable of handling multiple authorities were recently proposed by Chase. The scheme is built upon a single-authority attribute based encryption technique presented earlier by Sahai and Waters. [6]-[9] Chase's construction uses a trusted central authority that is inherently able to do decrypting arbitrary cipher texts created within the system. We present a multi-authority attribute based encryption technique in which only the set of recipients defined by the encrypting party can decrypt a corresponding cipher text. The central authority is shown as "honest-but-curious": on the one hand it honestly follows the protocol, and on the other it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. The advance scheme, which like its predecessors relies on the Bilinear DiffieHellman assumption, has a complexity comparable to that of Chase's technique. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority. Building on the proposal for multi-authority based attribute based encryption from; we constructed a scheme where the central authority is no longer capable of decrypting arbitrary cipher texts created within the system. In addition to viewing security in the selective ID model, we showed that the proposed system can able to tolerate an honest-but-curious central authority. Since both Chase's scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chase's construction. However, since the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is suggested in applications where security against such a central authority is required. [9]

3. Decentralizing Attribute-Based Encryption

AUTHORS: Allison Lewko, University of Texas at Austin alewko@cs.utexas.edu

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In this process, any party can become an authority and there is no requirement for any world coordination other than the innovation of an initial set of common reference parameters. A party can simply plays as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in forms of any Boolean formula over attributes issued from any chosen set of authorities [7]. Finally, our process does not require any central authority. In constructing our system, our largest technical hurdle is to create it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE technique authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. But in our system each component will come from a potentially different authority, where we think no coordination between such authorities. We create new techniques to tie key components together and prevent collusion issues between users with different global identifiers. We prove our system secure using the new dual system encryption methodology where the security proof works by first converting the challenge cipher text and private keys to a half-functional form and then arguing security. We follow a recent variant of the dual system proof scheme due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under same static assumptions to the LW paper in the random oracle model.

4. Accountable Authority Cipher text-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud AUTHORS: Jianting Nin , Xiaolei Dong , Zhenfu Cao and Lifei Wei [3]

As a sophisticated mechanism for secure well-grained access control, cipher text-policy attribute-based encryption (CP-ABE) is a highly promising solution for commercial applications like cloud computing. But there still exists one major issue awaiting to be solved, that is, the prevention of key abuse. The existing CP-ABE systems missed this critical functionality, hindering the wide utilization and commercial application of CP-ABE systems to date. Here we address two practical problems about the key abuse of CP-ABE: The key escrow problem of the half-trusted authority; and, The malicious key delegation problem of the users. For the semi-trusted authority, its misconduct (i.e., illegal key (re-)distribution) should be caught and prosecuted. And for a user, his/her malicious conduct (i.e., illegal key sharing) need be traced. We affirmatively solve these two key abuse issues by proposing the first accountable authority CP-ABE with white box traceability that supports policies expressed in any monotone access structures. And we provide an auditor to judge publicly whether a suspected user is guilty or is framed by the authority. In this process, we addressed two practical problems about the key abuse of CP-ABE in the cloud, and have presented an accountable authority CP-ABE technique supporting white-box traceability and public auditing. Specifically, the proposed system could trace the spiteful users for illegal key sharing. And for the half trusted authority, it's illegal key (re-)distributing misconduct could be caught and prosecuted. Furthermore, we have provided an auditor to judge whether a malicious user is naive or framed by the authority. As far as we know, this is the first CP-ABE technique that simultaneously encourages white-box traceability, accountable authority, public auditing. We have also proved that the new system is total protection in the standard model. Note that there exists a stronger notion for traceability called black-box traceability. In black-box scenario, the malicious user can hide the decryption algorithm by tweaking it, as well as the decryption key. And in this case, the advanced system with white-box traceability in this paper will fail since both the decryption key and decryption algorithm are not good. In our future work, we will focus on constructing an accountable authority CP-ABE technique which is black-box traceability and public auditing. [3]

III. Methodology

Step 1: In this project we are not only providing data content privacy, we are also providing identity privacy by using anonycontrol.

- AnonyControl decentralizes the central authority to limit the identity origin and thus achieves semi-anonymity. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity.

Step 2: In our system we use Attribute Encryption Standard (AES) algorithm. This algorithm is used to protect classified information and is used by the total world to encrypt and decrypt sensitive data.

AES consists of three block ciphers. AES-128, AES-192, AES-256 and this each cipher uses 128 bits of blocks using cryptographic keys 128,192 and 256 bits to encrypt and decrypt delicate data. So the ciphers uses same secret key for encrypting and decrypting. There are different rounds for keys. Each round consists of different steps include substitution, transposition and mixing of plain text. Finally the plain text is transformed into cipher text.

Step 3: In our system, there are four types of systems: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers.

A user can be a Data Owner and Data Consumer simultaneously.

- Data owner encrypt and uploads the files in to the cloud server. Data consumer decrypts and downloads the files from the cloud server.

Step 4: To access and perform any operations on files the data owner and data consumer should first register in to the system.

- When they registered at a time password and unique id will send to their registered mail id.

Step 5: To upload and download files by the user. The user may be a data owner and data consumer request the authority for permission.

- The authority provides public key to data owner and private key to consumer.

Issuing keys by authority and authentication in our system is succeeding using attribute based encryption. [1] [5]

Step 6: Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon (e.g. the country he lives, or the kind of subscription he has).

In such a system, the decryption of a cipher text is conceivable only if the set of attributes of the user key matches the attributes of the cipher text. A critical security aspect of Attribute-Based Encryption is collusion-resistance. An adversary that holds multiple keys should be able to access data if at least one individual key grants access.

Step 7: Using the keys provided by authority the users (data owner and data consumer) access the files in to and from the cloud server.

IV. IMPLEMENTATION

Implementation is the status of the project when the theoretical design is turned out into a working system. Thus it can be designed to be the most critical stage in achieving a successful new system and in giving the user, assurance that the new system will work and be effective. [4]

The implementation stage involves accurate planning, analysis of the existing system and it's constraints on implementation, designing of methods to attain changeover and estimation of changeover methods. [10]

MODULE DESCRIPTION:

After careful analysis the system has been classified to have the following modules:

1. Registration based Social Authentication Module

2. Security Module

3. Attribute-based encryption module.

4. Multi-authority module.

Fig:1 represents the architectural flow of the modules which we have used.

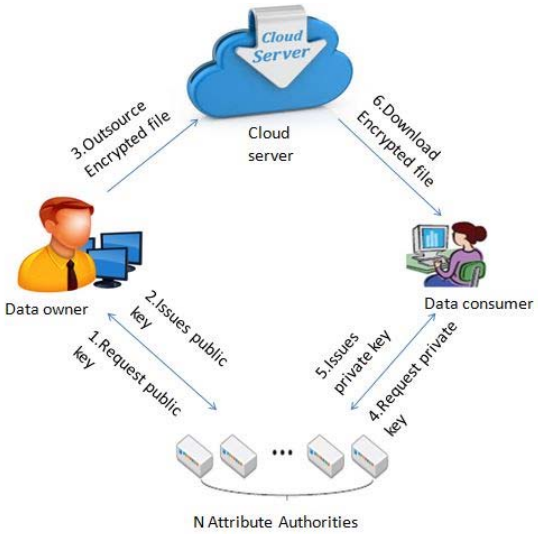


Fig: 1 Architectural Flow Diagram

1. Registration - Based Social Authentication Module

The system prepares executor for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few friends, who also have accounts in the system, are selected by either Alice or the service provider from Alice's friend list and are appointed as Alice's Registration. [1]

2. Security Module

Authentication is a key for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a confidential email being sent from your mail because someone had forged your information. Annoyed recipients and spam complaints resulting from it become your confusion to clean up, in order to repair your reputation. Guardian-based social authentication systems request users to select their own trustees without any constraint. In our experiments, we display that the service provider can constrain trustee selections by imposing that no users are selected as trustees by too many other users, which can achieve greater security guarantees

3. Attribute-based encryption module

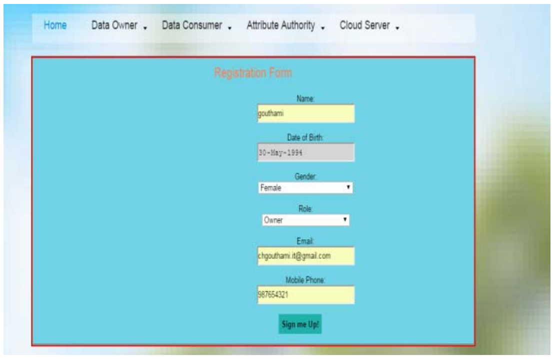
Attribute-based encryption module is adopting for each and every node encrypt data store. After encrypted data again the re-encrypted the same data is using for fine concept using user data uploaded the attribute-based encryption have been schemed to secure the cloud storage Attribute Based Encryption (ABE). In such encryption scheme, an identity is considered as a set of identifying attributes, and decryption is possible if a decrypted identity has some overlie with the one specified in the cipher text.

4. Multi-authority module

A multi-authority system is conferred in which each user has an id and they can collaborate with each key generator (authority) using different pseudonyms. Our goal is to attain a multi-authority CP-ABE which achieves the security defined above; secures the confidentiality of Data Consumers' identity information;[10] and tolerates compromise attacks on the authorities or the collusion intrusion by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

V. RESULTS

To upload and download files the data owner and consumer must be registered. Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. [1],[8],[9]



Registration Form

Name: gouthami

Date of Birth: 30-May-1994

Gender: Female

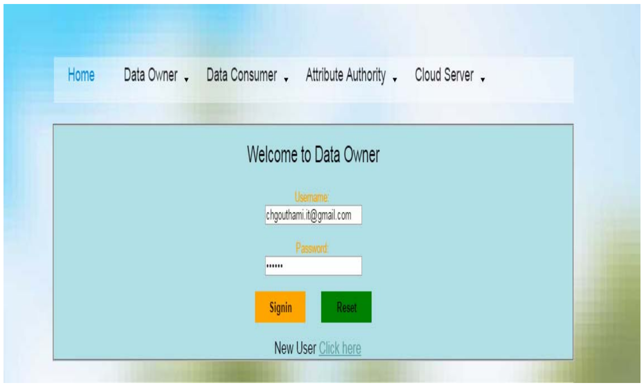
Role: Owner

Email: chgouthami.it@gmail.com

Mobile Phone: 987654321

When they registered is completed then password and unique id will be sent to registered mail ID.

Using this id and password they should login.



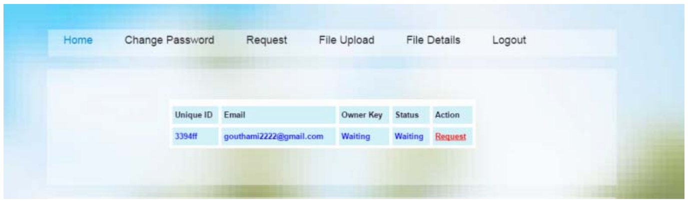
Welcome to Data Owner

Username: chgouthami.it@gmail.com

Password: ••••••

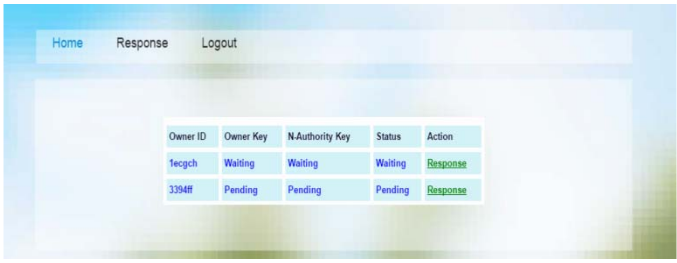
New User Click here

3. After this they have to request the authority for permission to perform operation on files.



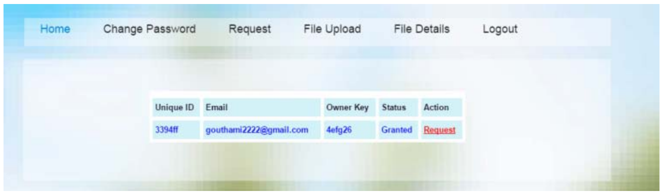
Unique ID	Email	Owner Key	Status	Action
3394ff	gouthami2222@gmail.com	Waiting	Waiting	Request

4. N-Authorities provide public key, authority key for owner and private key, authority key for consumer to perform operations on files.

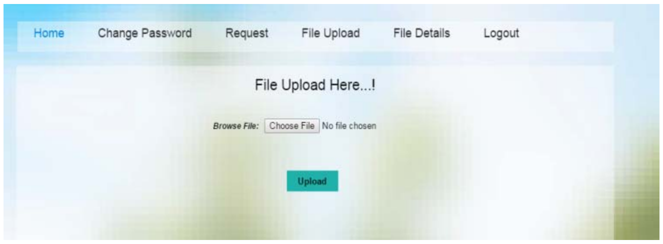


Owner ID	Owner Key	N-Authority Key	Status	Action
1ecgch	Waiting	Waiting	Waiting	Response
3394ff	Pending	Pending	Pending	Response

5. Using public key the data owner performs encryption and uploads files in to the cloud server.



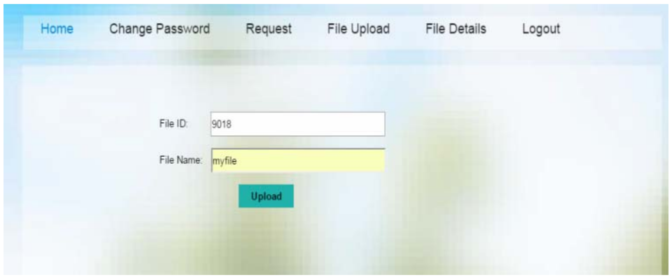
Unique ID	Email	Owner Key	Status	Action
3394ff	gouthami2222@gmail.com	4efg26	Granted	Request



File Upload Here...!

Browse File: Choose File No file chosen

Upload

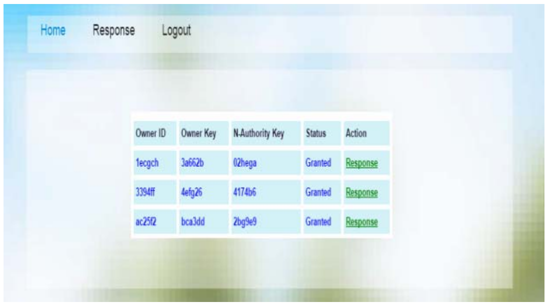


File ID: 9018

File Name: myfile

Upload

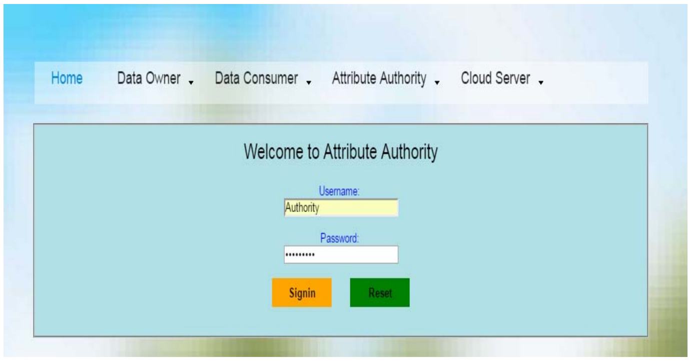
6. Using private key the data consumer performs decryption and downloads files from the cloud server.



Owner ID	Owner Key	N-Authority Key	Status	Action
1ecgch	3a662b	02hega	Granted	Response
3394ff	4efg26	4174b6	Granted	Response
ac25f2	bca3dd	2bg9e9	Granted	Response

7. Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the cipher text.

8. A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above guarantees the confidentiality of Data Consumers' identity information.

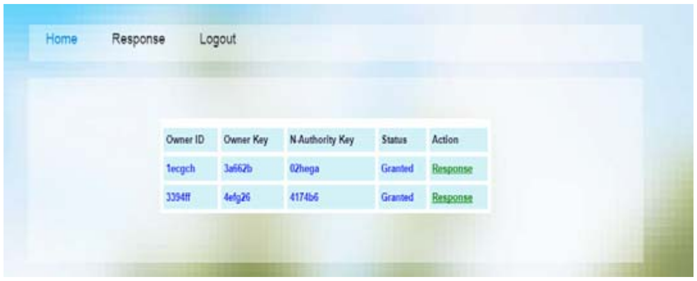


Welcome to Attribute Authority

Username: Authority

Password: •••••••••

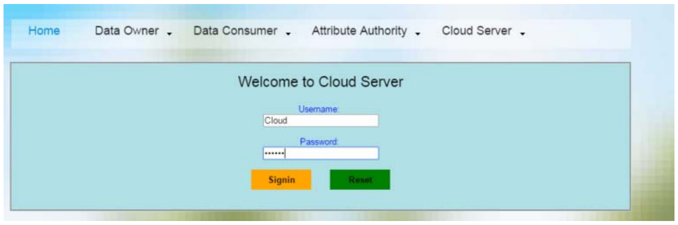
Signin Reset



Owner ID	Owner Key	N-Authority Key	Status	Action
1ecgch	3a662b	02hega	Granted	Response
3394ff	4efg26	4174b6	Granted	Response

9. At the cloud server all the data is in encrypted form the cloud server is unable to see the details and data.

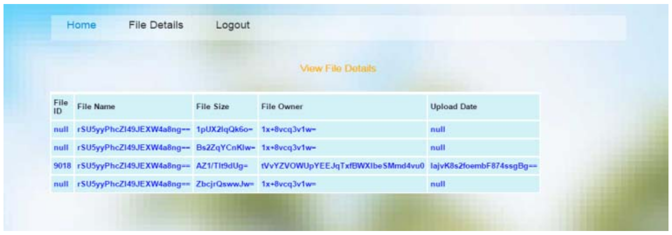
By which we are providing not only providing data privacy but also user identity privacy by anonymity with fully anonymous attribute based encryption.



Welcome to Cloud Server

Username: Cloud

Password: ••••••



View File Details

File ID	File Name	File Size	File Owner	Upload Date
null	rSU5yyPhcZI49JEXW4a8ng==	1pUX2lqQk6o=	1x+8vcq3v1w=	null
null	rSU5yyPhcZI49JEXW4a8ng==	Bs2ZqYCnKlw=	1x+8vcq3v1w=	null
9018	rSU5yyPhcZI49JEXW4a8ng==	AZ1/Tlt9dUg=	tVvYZVOWUpYEEJqTxfBWXlbeSMmd4vu0	lajvK8s2foembF874ssgBg==
null	rSU5yyPhcZI49JEXW4a8ng==	ZbcjrQswwJw=	1x+8vcq3v1w=	null

VI. CONCLUSION

This paper introduces 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. By using the multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while controlling privilege control based on users' identity information. More importantly, our system can accept up to N −2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also direct detailed security and performance analysis which shows that AnonyControl both efficient and secure for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it. One of the upcoming future works is to introduce the efficient user repudiation mechanism on top of our anonymous ABE. Supporting user repudiation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. [11] Making our schemes adaptable with existing ABE schemes support efficient user revocation is one of our future works.

ACKNOWLEDGMENT

We wish to thank MLRIT College for providing eminent facilities to initiate our research. It is pleasure to express my profound gratitude to Dr. K.V.S.N Ramarao, Mrs. B. Madhuravani Assoc Professor, K. Sai Prasad Asst. Professor for continuous support in understanding the problems and correcting us wherever required. It's my pleasure to thank my friend K. Gouthami, for their support in completion of this work successfully.

REFERENCES

[1] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan," Cipher text-Policy Attribute-Based Encryption", T Jung - 2015.

[2] 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings.

[3] White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes Jianting Ning, Xiaolei Dong, Zhenfu Cao, Senior Member, IEEE, Lifei Wei, and Xiaodong Lin, Senior Member, IEEE

[4] 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part 2.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO. Springer, 1985, pp. 47–53.

[6] Frederic P.Miller,Agnes F.vandome,John McBrewster," Advanced Encryption Standard,2009,ISBN:6130268297 9786130268299.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT. Springer, 2005, pp. 457–473.

[8] "Decentralizing Attribute-Based Encryption" Allison Lewko, University of Texas at Austin alewko@cs.utexas.edu

[9] Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi. "Multi-authority attributes based encryption with honest-but-curious central authority".

[10] S. G. Akl and P. D. Taylor. Cryptographic Solution to a Multi Level Security Problem in Advances in Cryptology -- CRYPTO 1982.

[11] M.R.KAVITHA RANI,M.E, S.BRINDHA, M.E., "A Survey on Data Stored in Clouds" ISSN: 2350-0328 International Journal of Advanced Research in Science, Engineering and Technology Vol. 2, Issue 11 , November 2015