iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

CRA Role in Identity-Based Encryption for Its Applications

Ashok J Yede[1], Prof. V. S. Nandedkar[2]
[1,2] Department of Computer Science and Engineering PVPIT, Bavdhan Pune-21, India

Abstract: ***Identicalness based Cryptography is an id based cryptography which depends on the user identity, (IBE) is a world Key cryptoorganisation and eliminates the need of public paint infrastructure (PKI) and certicate administration in conventional public key context. Due to the absence of PKI, the revocation problem is a critical yield in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. There are two issues of revocation in existing system first one is a revoking and computation monetary value is higher and second one is KU-CSP servers scalability, because KU-CSP need to keep a mystery value of each user, for that purpose system invented a Cloud Service Authority (CRA) used instead of KU-CSP Server to solve the shortcomings of the existing system and handling a burden of the PKG server. In this CRA only need to hold systems secret value. In this paper we proposed distributed cloud computing by separating CRA and PKG servers. Layered approach will be used on both the server.***

Index Terms—cloud computing, Identity-based encryp- tion(IBE), Revocation, Outsourcing, CRA, PKG.

I. INTRODUCTION

Indistinguishability -based Encryption (IBE) provides an important alternative way to avoid the need for a world key infrastructure (PKI). Revocation capability is very important for IBE stage set as well as PKI solidification. Identity (ID)-based encoding , or IBE for short, is an exciting alternative to populace -key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that make publicly available the mapping between identicalness , public key , and validity of the latter. The senders using an IBE look ups the public keys of the receivers, because the identities (e.g. email or IP addresses) together with common public parametric quantity are sufficient for encryption. The private keys of the exploiter are issued by a trusted third company called the private key author (PKG). Ideas of identity element -based cryptography go book binding to 1984 and Shamir [6], but the First IBE scheme was constructed by Boneh and Franklin only in 2001 [VI], construction on the progress in elliptic curves with bi-linear pairings. Any setting, PKI- or identity-based, must provide a means to renege exploiter from the system of rules, e.g. if their private keys get compromised. In a PKI setting a certification authority informs the senders about expired or revoked keys of the users via publicly available digitalsecurity s and certificate revocation listing.

Though IBE allows an arbitrary cosmic string as the public Key which is considered as appealing advantages over PKI, it demands an efficient revocation mechanism. Specifically, if the private Florida key of some user gets compromised, we must provide a mean to revoke such substance abuser from arrangement. In PKI stage set , revocation mechanism is realized by appending validity geological period to certificates or using involved combinations of proficiency [2][3]. Nevertheless, the cumbersome management of certificates is precisely the load that IBE strives to alleviate. As far as we know, though revocation has been thoroughly written report in PKI, few revocation mechanisms are known in IBE setting. In [5], Boneh and Benjamin Franklin suggested that exploiter renew their private key periodically and senders use the receivers identicalness concatenated with stream time period. But this mechanism would result in an operating cost load at PKG. In another word, all the drug user regardless of whether their identity have been revoked or not, have to contact with PKG periodically to prove their identities and update new private secrete personal Key. It requires that PKG is on line and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the system grows or number of users grows.

II. REVIEW OF LITERATURE

A. Identity-Based Encryption with Cloud Revocation Authority and Its Applications

This paper is focusing the two basic issues of performance and scalability.Author provides Cloud Revocation Author- ity(CRA) replacement for KU-CSP. KU-CSP was holding time update key for each and every user. It was separate and hence scalability issue observed for large number of users. Also, There was only one KU-CSP server which was becoming bottleneck for performance, and hence author proposed a CRA. And there can be multiple CRA on the basis of load. If there are lot of load on

system, then by using load balancing multiple CRA serves end user request.

B. Identity-based Encryption with Outsourced Revocation inCloud Computing

In this paper, author focusing on the critical issue of identity annulment, author introduced outsourcing generation of key into IBE and propose a revocable scheme in which the revocation cognitive operation are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-of- the-moon -featured: 1) It achieves constant efficiency for both computation at PKG and private Florida key size at substance abuser; 2) User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline/powersaving mode after sending the revocation list to KU-CSP; 3) No secure channel or user authentication is required during key-update between user and KU-CSP.

C. Efficient revocable ID-based encryption with a public channel

Tseng and Tsai in 2012 came up with new revocable IBE scheme. This is to remove the usage of secure channel between each user and with the authority, user uses the public channel; instead of using to transmit users' regular private keys. Author divides the user's private key into two components, as ,an identity key and a regular time update key. The identity key is a secret key for a specific user's ID, which is sent to the user via a secure channel and remains unchanged since being issued. The time update key is a key associated with user's ID and time period, which is changed along with time. The PKG periodically generates current time update keys for non- revoked users and sends them to these users via a public channel.

D. Adaptive-ID Secure Revocable Identity-Based Encryption.

Identity-Based Encoding (IBE) offers an interesting option to PKI-enabled encryption as it eliminates the need for digital credential. While annulment has been thoroughly cogitation in PKIs, few revocation mechanisms are known in the IBE setting. Until quite recently, the most convenient one was to augment identities with period numbers at encryption. All non-revoked pass receivers were thus forced to obtain a new decryption winder at discrete clock time intervals, which places a significant burden on the authorization [9]. More efficient method acting was suggested by Boldyreva, Goyal and Kumar at CCS'08. In their revocable IBE scheme, key updates have logarithmic (instead of linear in the original method) complexity for the trusted authority.

E. Privacy-preserving Attribute Based Searchable Encryption

The nameless ABE provides interesting safety characteristic receiver anonymity further to information confidentiality and ne-grained gets right of entry to control of ABE. While storing encrypted files in public cloud, green search capability helps consumer to retrieve a subset of documents for which the consumer has get admission to rights on stored documents. We proposed an anonymous attribute based searchableencryption (A2SBE) scheme which helps user to retrieve only a subset of files referring to his selected keyword(s). User can add documents in public cloud in an encrypted shape, search files based on keyword(s) and retrieve files without revealing his identity. The scheme is established cozy under the standard antagonistic version. The scheme is efficient, as it requires small storage for user's decryption key and decreased computation for decryption in assessment to different schemes.

III. EXISTING SYSTEM

Following Fig. 1 shows revocable IBE scheme for PKG severs. Existing system consist of CRA and a PKG servers. PKG server is responsible to generate user's private key for encryption. CRA server is responsible to generate user's public identity key for encryption. CRA server also generates periodic time update key for each user and applies it for all users. If any user to revoke, CRA just stops to generate and sends that time update key to end user. CRA maintains single master time key for time update key generation for all users.

Initially PKG server starts to generate new private key for user and then CRA server generates the time update key for the same user. Once the private and pubic keys are available for end user, then end user can start using them in any system for encryption and decryption. These keys are generated from users identity. User identity can be any users mobile number or email address. This system can have multiple CRA's but single PKG server. As they are providing single master time key, it resolves the scalability issue. Also, as system has multiple CRA servers, it also reduced performance issue to some extent.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

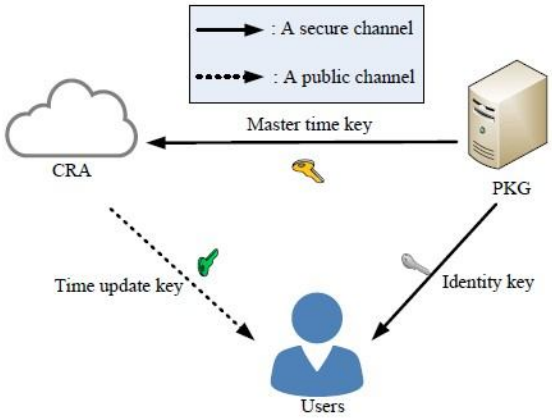


Fig. 1. Existing System

Abbreviations and AcronymsKU-CSP: Key Update Cloud Service Provider
CRA: Cloud Revocation Authority
PKG: Private Key Generator IBE: Identity Based Encryption PKI: Public key infrastructure UI:
User InterfaceBL: Business Layer
DAL: Data Access Layer
DB: Database server

IV. PROBLEM STATEMENT FOR EXISTING SYSTEM

A. Performance: Single PKG server is used for private key generation and hence dependency on same server is too high. It also has all things required for CRA server on single server, can be improved.
B. Scalability: KU-CSP needs to maintain the time key list for all the users and hence it increase management load.

V. SYSTEM ARCHITECTURE

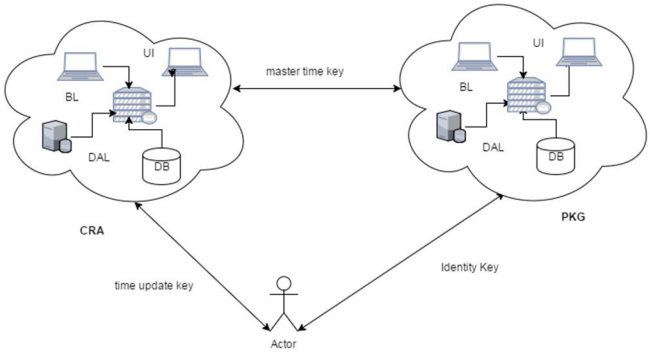


Fig. 2. System Model

As Shown in a above Fig 2., to overcome the disadvantages of an existing scheme, In rules of order to solve both the un-scalability and the inefficiency we proposed a new revocable IBE scheme with cloud revocation authority(CRA), we have invented. Private tonality's of the user's consist of identity fruitful key and fourth dimension update key. The System of rules introduces a new CRA server, as the alternate of KU-CSP. And also, introduced distributed and layered system structures and approaches. In this system CRA grip a randomly generated master key to generate time update key. This master key is used for generating a time update key time periodically, for a non-renege users and sends that time update key through the user mail id. Our scheme uses the multiple CRA as well as PKG servers. Our scheme also solves the problem of KU-CSP (un-sclability).
As shown in System architecture diagram, system consist of basically again two servers. Proposed system consist of multiple

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

PKG servers to remove the bottleneck of PKG server. As PKG server is used to generate private key for each user, we are proposing multiple PKG servers to improve perfor- mance. CRA server functionality is distributed with layered approaches. By using layered approach, we tried to reduce the load on single server. We are distributing the single server load to multiple servers on the basis of actual business use and functionality. Single server can be divided in to Database,

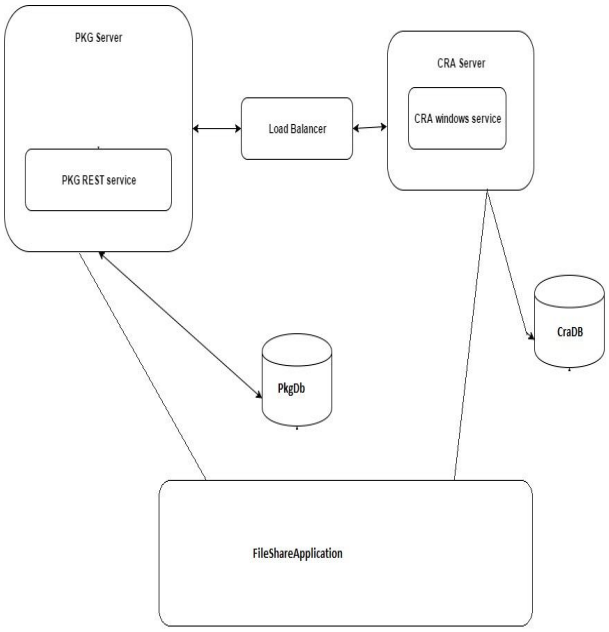


Fig. 3. Detailed System Model

business layer and data access layer. Same layered approache is proposed for PKG server as well.

VI. MATHEMATICAL MODEL

Mathematical model represents the complete system with all possible inputs and outputs. I1 to I5 are the inputs as explained below and O1 to O5 are the outputs. Let 'S' be the system to perform A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud.

S= I, O, F, Fail, Success
Where, Inputs I := I1, I2, I3, I4, I5
I1 := Master Secrete Key
I2 := User Identity Key
I3 := Request To The Group Manager
I4 := Access Policies
Where O is a Output
Output O = O1, O2, O3, O4, O5
O1 := Generated Secrete Key
O2 := Upload File
O3 := Encryption Of Data
O4 := Decryption
O5 := Download File
Functions set F := f1, f2, f3, f4, f5, f6
f1 := Setup
f2 := Key Generation f3 := Upload file
f4 := Encryption f5 := Decryption
f6 := Revocation Of User

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Failure Conditions: If user doesn't receive required time update key and private key for non revoked user. If revoked user access encrypted data

Success Conditions: For Every user secret time update key and private key is generated by a group manager. Access policies should assign properly so particular user access a file.

VII. SYSTEM ANALYSIS

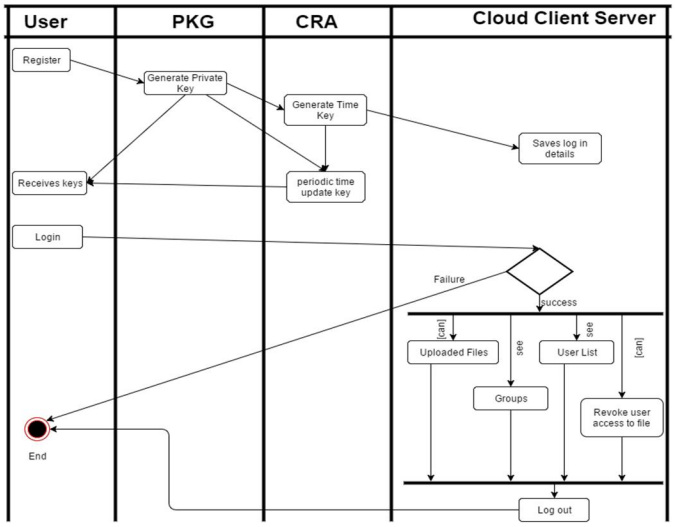


Fig. 4. Activity Diagram

System is divided as distributed system. Each of these distributed servers or modules will contain layered approach. Basically there will be three layers UI, BL and DB as shown in system architecture diagram. System Components:

A. CRA

Maintain a common secret key for all users, generates a time update key for user whenever is requesting new user registers, time span. User revocation can be done by the CRA. System can have multiple CRA servers with layered approach

B. PKG

This module generates identity private key send identity p key to the user and master key which will send to CRA for a user which is secret random value .

C. User

This module will give the facility for register a user and login.

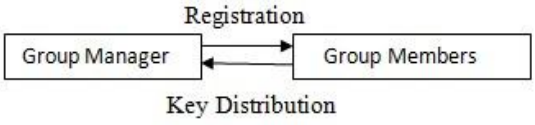


Fig. 5. Registration

After registration user can login to system. Periodically CRA updates time update key and revoke user to access uploaded files. PKG sends updated user revocation list to CRA and CRA revoke these users. Revoked users can not access encrypted data from system.

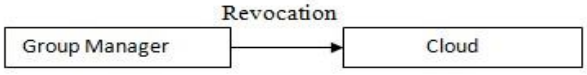


Fig. 6. User Revocation

D. File Creation and Deletions

Registered user can upload his own data to the system and will define the access to the system. And hence he will delete and will able to create/upload new file to the system.

E. File Access

To access any specific file from any group, user needs to request access to group manager. Group manager will grant or deny the access.

VIII. PERFORMANCE RESULT AND ANALYSIS

We user Sample data from limited user registration to the system We use Microsoft Azure to deploy the system using load testing we test the services and their response time

A. User Registration

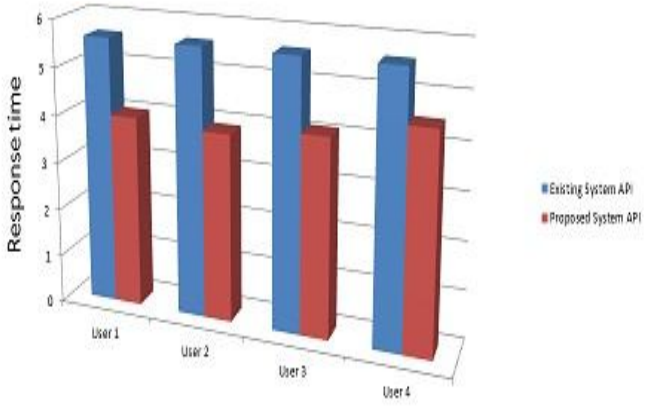


Fig. 7. Time Update Key Response Time

B. Modules

To use proposed system, user need to register in to system. System will ask some basic details and his identity to differentiate user from other users. User name or email id or phone number can be one of the user identity that can be used as a unique. Then group manager adds this registered user to access the group contents.

C. User Revocation

Following are our observations

Distributed systems improves the performance

1) Load Balancer handles API requests and passes to respective vserver

2) Layered approach is used to reuse and distribute the system components

3) PKG bottleneck is removed by using distributed and layered approach systems

IX. CONCLUSION

The proposed System Revocable outsourcing IBE system is completely based on the CRA Authorisation, In this system a revocation is performed by CRA for handling an effect of a PKG server, then the CRA Host generates a master meter key fruit and sends that to the user so the integrity of the filing cabinet should be maintain, Whenever the receiver request for file, Every fourth dimension a new master time key will be generated for a particular user. Distributed and layered approach is also very fruitful to resolve the existing system problems in IBE.

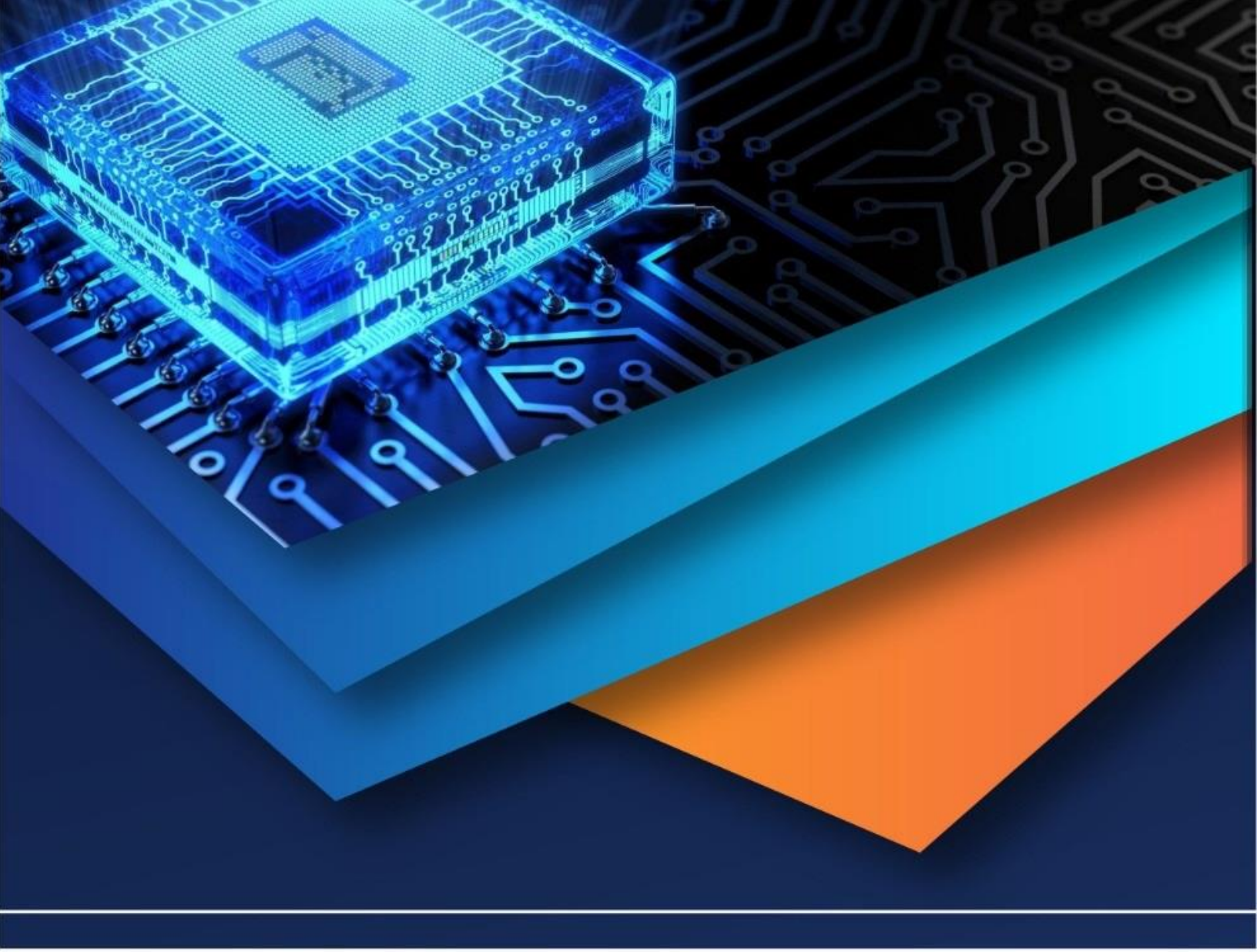
X. ACKNOWLEDGMENT

I would like to thank to Prof.V.S.Nandedkar for her precious comments. It is my privileges to acknowledge with deep sense of gratitude to her for valuable suggestions and guidance to understand the system and to resolve the problem.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

REFERENCES

[1] Yuh-Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang, Identity-Based Encryption with Cloud Revocation Authority and Its Applications, Proc. Crypto84, LNCS, vol. 196, pp. 47-53, 1984.G.
[2] A. Shamir, Identity-based cryptosystems and signature schemes, Proc. Crypto84, LNCS, vol. 196, pp. 47-53, 1984.G.
[3] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Proc. Crypto01, LNCS, vol. 2139, pp. 213-229, 2001.
[4] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, Identity-based encryption with outsourced revocation in cloud computing, IEEE Trans. O Computers, vol. 64, no. 2, pp. 425-437, 2015.
[5] Y.-M. Tseng. and T.-T. Tsai, Efficient revocable ID-based encryption with a public channel, Computer Journal, vol.55, no.4, pp.475-486, 2012.
[6] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, Identity-based encryption with outsourced revocation in cloud computing, IEEE Trans. On Computers, vol. 64, no. 2, pp. 425-437, 2015
[7] A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with efficient revocation, Proc. CCS08, pp. 417-426, 2008.
[8] Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based Encryption for fine-grained access control of encrypted data, Proc. ACM CCS, pp. 89-98, 2006
[9] B. Libert and D. Vergnaud, Adaptive-ID secure revocable identity-based encryption, Proc. CT-RSA09, LNCS, vol. 5473, pp. 1-15,2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY