Controlled Data Access Using IBE in Cloud Computing

Bhoomika M U, Chandini M, Harshitha.R.S, Suraj S Gurav, Prof. Mangala.C.N
UG SCHALOR, Associate Professor
Department of CS&E,
East West Institute of Technology, Bangalore, India
bhoomi123mu@gmail.com, chans.1994@gmail.com, harshithasiddesh93@gmail.com, guravsuraj@gmail.com
mangalacn@ewit.edu

Abstract – Identity Based Encryption or Identity based encryption is an important primitive of ID-Based Cryptography. It is an important alternative to public key encryption. Identity based encryption which simplifies the public key and certificate management. Propose a revocable Identity based encryption scheme in the server aided setting. It is achieved by utilizing a novel collusion resistant technique which means generating a hybrid private key for every user using AND gate it helps to connect and bound the identity and time component. In this paper aiming at tackling the critical issue of identity revocation we introduced the outsourcing revocation for the first time and the purpose of revocable IBE scheme in server aided sitting. Our scheme offloads most of the generation related operations during key issuing and key update process to a key update cloud service provider, leaving only a constant number of simple operations for PKG and user to perform locally. This goal is achieved by utilizing a novel collusion resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore it gives a secure under the recently formulised refereed delegation of computation model. Finally we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Index terms-Identity based encryption, key generation, cloud computing.

1. INTRODUTION

Identity based encryption is an important primitive of ID-based cryptography. As such it is a type of public key encryption in which the public key of a user is some unique information about the identity of the users (e.g. a user‗s email address).this means that a sender who has to the public parameters of the system can encrypt a message using e.g. the text-value of receiver‗s name or email address as a key .the receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.

IBE was proposed by Adi Shamir in 1984.he was however only able to give an instantiation of identity based signatures. Identity based encryption remained an open problem for many years .The pairing based Boneh-Franklin scheme and cock‗s encryption scheme based on quadratic residues both solved the IBE problem in 2001.

IBE system allows any party to generate a public key from a known identity value such as an ASCII string .A trusted third party, called the private key generator ,generates the corresponding private keys .To operate ,the PKG first publishes a mater public key and retains the corresponding master private key. Given the master public key ,any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value .To obtain a corresponding private key the party authorized to use the identity ID contacts the PKG ,which uses the master private key to generate the private key identity ID.

As a result, parties may encrypt messages with no prior distribution of keys between individual participants. This is extremely useful in cases where Pre distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG.

2. LITERATURE REVIEW

Identity based encryption is an arousing curiosity modification for public key encryption, it is generated to compute the key management in a certificate based public key infrastructure using user information such as name email ID , address etc and it is considered as public key. So that we can tell that, public key and certificate is not necessary for the sender using IBE, But using a receiver identity we can directly encrypt the message.

With the corresponding identity, receiver obtaining the private key from the private key generator and PKG is used to decrypt the ciphertext.

An arbitrary string is used as public key for the IBE, is represented as an advantages of against PKI, which demands for the accurate revocation technique.

Server revokes the users from the system when the private keys of user get expired. Revocation is based on validity period for certificates

Boneh and Franklin are the first implementers, IBE was researched by using a cryptographic application.

Security was proven in random oracle for the first model. Under the selective ID and adaptive ID some subsequent systems are achieved provable secure, now a days for the IBE systems there have been number of lattice based constructions are presents. Boneh and Franlin‗s were given more suggestions but it is impractical.

Hanaoka et al. implements that, users should renew their own secrete keys periodically when without communicate with the PKG. in this work every user should possess a tamper resistant device. And here it has one more solution is that: mediator aided revocation means there is a trusted third party to supports users to decrypt the all ciphertext.

Lin et al. proposed A Space efficient revocable IBE techniques from ABE but it requires bilinear operations for a single decryption.

Libert and vergnaud improved the revocable IBE schemes and they focused on the enhancement of security.

3. PRELIMINARY

Cryptographic background:
Bilinear Map: e: $G_1 \times G_1 \rightarrow G_2$.

- G_1, G_2 are cyclic groups of same prime order p:
- G_1: Additively G_1=(p);
- G_2: Multiplicatively written.

Known examples: weil and tate pairings.
G_1: Subgroups of an elliptic curve group.
G_2: Subgroups of the multiplicative group of a finite field.

Bilinear Map: Properties
Bilinearity: e(aP,bP)=e$(p,p)^{ab}$.
Non –degeneracy: e(p,p)≠1.
DBDH: using of this advantages are
Let A be a probabilistic algorithm
Input: (P, P_1 ,P_2 ,P_3, Z) $\in G_1^4 \times G_2$;
Output: a bit b (denoted by =A→b).

4. IDENTITY BASED ENCRYPTION

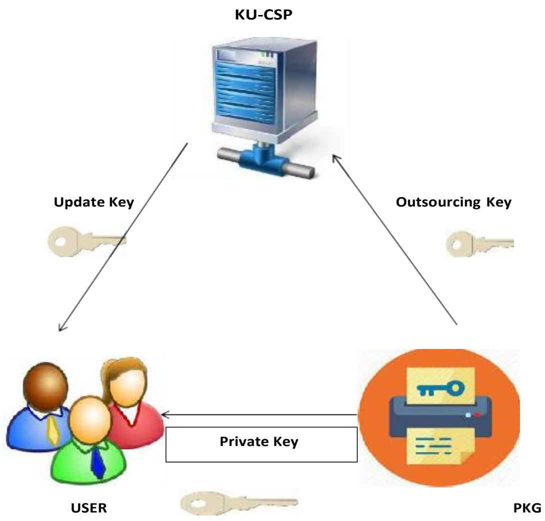


Fig.1. model of KU-CSP

Identity based encryption it consists of 4 algorithms that forms a complete IBE system:
Setup: this algorithm is run by the PKG one time for creating the whole IBE environment. The master key is kept secret and used to derive user‘s private keys, while the system parameters are made public .It accepts a security parameters k (i.e. binary length of key material) and outputs:
1.A set *P* of system parameters, including the message space and ciphertext space *M* and *C*.
2. A master key *Km*,
Extract: This algorithm is run by the PKG when a user requests his private key .Note that the verification of the authenticity of the requestor and the secure transport of *d* are problems with which IBE protocols do not try to deal .It takes as input *P*,*Km* and an identifier
ID ∈ $\{0,1\}^*$ and returns the private key *d* for user *ID*.
Encrypt: Takes *P*, a message *m* ∈ *M* and *ID* ∈ $\{0,1\}^*$ and output the encryption *c* ∈*C*.
Decrypt: Accepts *d*,*P* and ∈*C* and returns *m* ∈*M.*

5. PROBLEM STATEMENTS:

KU-CSP is used to realize the revocation for compromised users. KU-CSP can be used as a public cloud run by a third party to deliver basic computing capabilities to PKG as standardized services over the network. Revocation is triggered, instead of requesting private keys from PKG is unrevoked user.
How does Alice regain her privacy?
Basic idea: double encryption: combine a PKE and an IBE many subtleties to take care of.
The steps involved in the depicted in this diagram: Identity based encryption: Offline and Online.

Security definition:
Game between adversary and simulator.
Set-up: simulator

- Generates pp and master key.
- Provides the adversary with PP.
- Keeps master key secret.

Phase 1: adversarial queries.

- Key extraction oracle: ask for the key of my identity.
- Decryption oracle: ask for the decryption of any ciphertext on any identity.
- Restraction: cannot ask for decryption using ID, if a key ID has been asked earlier.

Challenge:

- Adversary outputs and two equal length message M_0 and M_1.
- Adversary should not have asked for the private key of ID*.
- Simulator chooses a random bit b; encrypts M_b using ID* to obtain C^*; Gives C^* to the adversary.

Phase 2: adversarial queries.

- Same as phase1.
- More restrications:
  Can‘t ask for the private key of ID*;
  Can‘t ask for the decryption of C* under ID*.

Advantage: $\in = \times P_r| \; b'] \; {}^1/_2|$.
$(\in, t)$-adversary: running time t: $\in$.

- Storage definition:

Full model: adaptive –ID and CCA- secure.

- Weaker definitions:
- Adaptive –ID and CPA-secure.
  Adversary not provided with the decryption oracle.
- Selective –ID
  Adversary has to commit to the target identity even before the protocol is set up.
  CPA-secure.
  CCA-secure.

Revocable IBE and security: An identity based encryption with efficient revocation or simply revocable IBE scheme *RIBE=(S,SK,KU,DK,ϵ,D,R)* is defined by an algorithms and has associated message space M , identity space I and time space T. we assume that of T is polynomial in the security parameter. Each algorithm is run by either one of three types of parties-key authority, sender or receiver.

Key authority maintains a revocation list rl and state st. Revocation list rl can be a part of state st, but we keep it explicit for clarity.

- Stateful setup algorithm S(run by key authority) takes input parameter 1^k and number of users n, and outputs public parameter p^k,master key mk, revocation list rl(initially empty)and state st.
- The stateful private key generation algorithm SK(run by key authority)takes input public parameter pk, master key mk ,identity $\omega \in$ I and state st. and outputs private key sk_w and an update state st.
- The key update generation algorithm Ku(run by key authority) takes input public parameters pk ,master key mk, key update time $\in$T, revocation list rl and state st, and outputs key update ku_t.

Security of revocable IBE

We define the selective revocable ID security for Revocable IBE scheme .our security model captures the standard notation of selective –ID security but it also takes into account possible revocations. Since we explicitly consider time period, in the beginning of the experiment in addition to the challenge identity the adversary also declares the challenge time. Just as in the standard selective –ID security definition the adversary can request to learn user‘s keys. In addition we let the adversary to revoke users of its choice at ant period of time and all key updates.

Unlike in the standard security model, we allow the adversary to learn the private key for the challenge identity, but only if it was revoked prior to or at the challenge time .the adversary given a ciphertext of one of the two messages of is choice encrypted for challenges identity and time. It has to guess which of the messages was encrypted.

First we define (selective) security against chosen –plaintext attack and then show how to extend the definition to chosen –ciphertext attack.

6. SYSTEM ARCHITECTURE

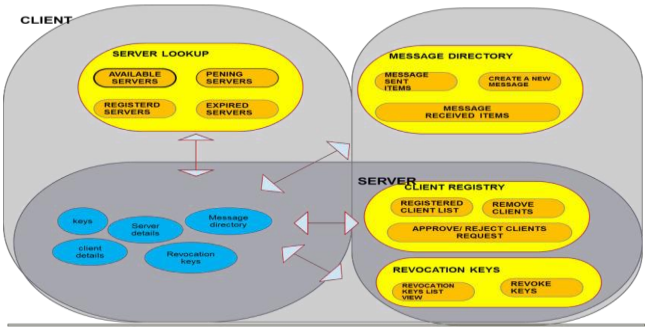


Fig.2. architecture diagram

Available servers: servers currently available for communication.

Register server: To preserve the connection information.

Expired server: whose register key has got expired.

Registered client list: list of clients who are registered with the server.

Remove client: remove the clients from the list whose key has got expired.

Approve/reject client request: approve or reject client request based on the request made by the client.

Client details: details of the server responses stored in the client.

Message sent items and message received items: number of and details of messages received and sent between client and server. details: details of the requests and messages sent by the client.

Revocation keys: Used to provide access privileges.

7. MAIN CONSTRACTION

In our IBE scheme message are encrypted for two –attributes‖: identity of the receiver and time period. The decryption key is also computed for attributes identity and time, on a first – degree polynomial, meaning both attributes of the decryption key must match with those of a ciphertext in order to decrypt.

We split the decryption key in two components corresponding to identity and time that we call private key and key update respectively.

The private key is issued to each user by the key authority just like regular private key in IBE. The key update is published by the authority and publicly available to all users.

8. PERFORMANCE ANALYSIS

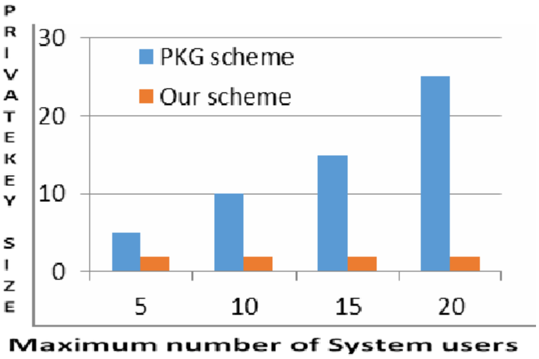
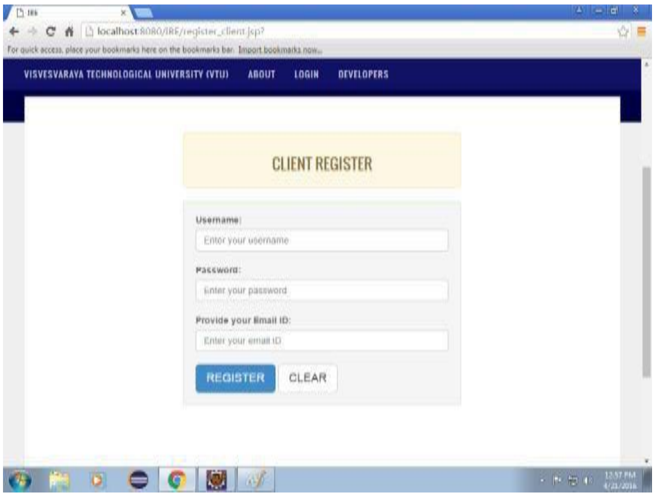


Fig.3. performance comparison

In this section, we will provide a thorough experimental evaluation of the construction proposed. In the above figure, we show the comparison on private key size. Besides the better performance in efficiency and private key size, another advantage of our scheme over the previous work is that it supports dynamic number of users. Specifically, the previous work requires to fix the maximum number of users in system initially to facilitate building the binary tree. Once the maximum number is fixed, it is difficult to add users exceeding this bound. Ours does not have such a drawback, and flexibly supports dynamic management of users.

9. SNAPSHOTS

Client Registration:


IBE
localhost:8080/IBE/register_client.jsp?
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
VISVESVARAYA TECHNOLOGICAL UNIVERSITY (VTU)
ABOUT
LOGIN
DEVELOPERS
REGISTER
CLEAR

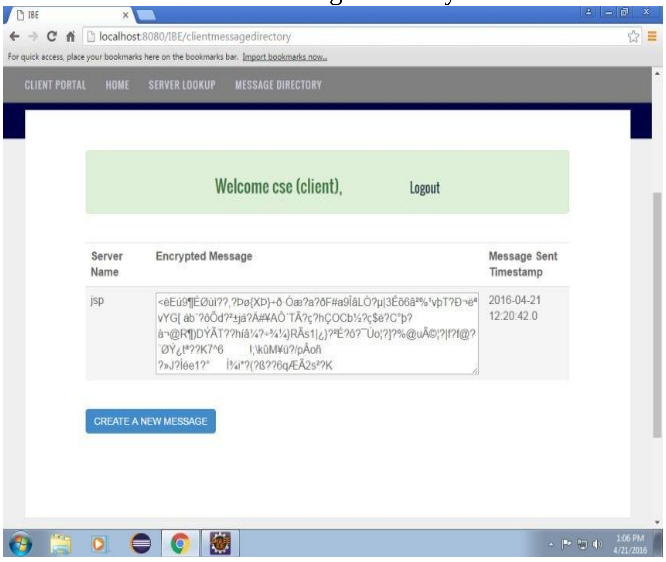
CLIENT REGISTER

Username:
Enter your username

Password:
Enter your password

Provide your Email ID:
Enter your email ID

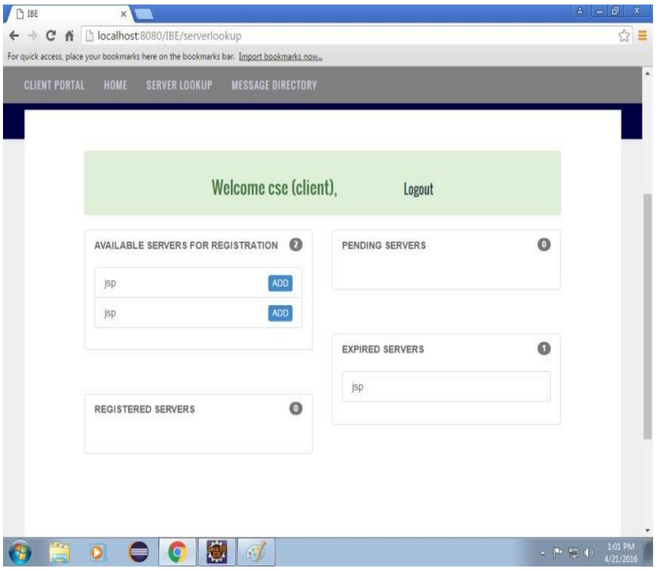
Client message directory:


IBE
localhost:8080/IBE/clientmessagedirectory
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
CLIENT PORTAL
HOME
SERVER LOOKUP
MESSAGE DIRECTORY
Logout
CREATE A NEW MESSAGE

Welcome cse (client),

Server Name	Encrypted Message	Message Sent Timestamp
jsp	<ëEû9¶ÈØùi??,?Þø{XÞ}÷ð·Óæ?a?ðF#a9ÎâLÒ?µ|3Êõ6ã²%¹vþT?Ð¬ëª vYG[áb´?õÕd?²±já?Ä#¥AÔ˙TÃ?ç?hÇOCb½?ç$ë?C°þ? à¬@R¶)DÝÃT??híâ¼?÷¾¼)RÃs1|¿}?²É?ô?¯Üo¦?]?%@uÃ©¦?|f?f@? ¨ØÝ¿tª??K7^6 !,\kûM¥ü?/pÅoñ ?»J?Ìée1?° Ì¾i*?(?ß??6qÆÃ2s²?K	2016-04-21 12:20:42.0

Server lookup:


IBE
localhost:8080/IBE/serverlookup
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
CLIENT PORTAL
HOME
SERVER LOOKUP
MESSAGE DIRECTORY
Logout
ADD
ADD

Welcome cse (client),

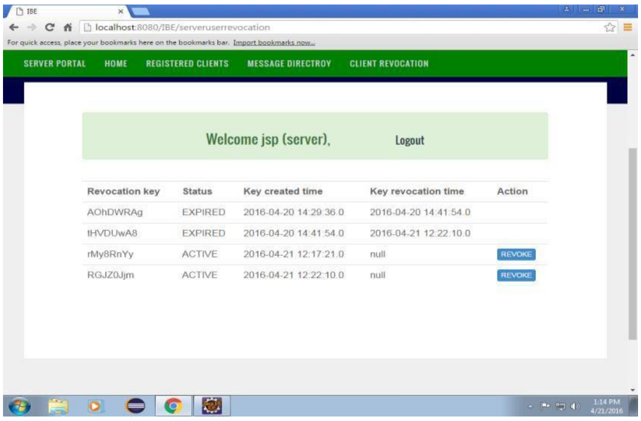
AVAILABLE SERVERS FOR REGISTRATION 2
jsp
jsp

PENDING SERVERS 0

EXPIRED SERVERS 1
jsp

REGISTERED SERVERS 0

Server user revocation:


IBE
localhost:8080/IBE/serveruserrevocation
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
SERVER PORTAL
HOME
REGISTERED CLIENTS
MESSAGE DIRECTROY
CLIENT REVOCATION
Logout

Welcome jsp (server),

Revocation key	Status	Key created time	Key revocation time	Action
AOhDWRAg	EXPIRED	2016-04-20 14:29:36.0	2016-04-20 14:41:54.0	
tHVDUwA8	EXPIRED	2016-04-20 14:41:54.0	2016-04-21 12:22:10.0	
rMy8RnYy	ACTIVE	2016-04-21 12:17:21.0	null	REVOKE
RGJZ0Jjm	ACTIVE	2016-04-21 12:22:10.0	null	REVOKE

10. CONCLUSION AND FUTUREWORK

Providin a critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-featured:

1) It achieves constant efficiency for both computation at PKG and private key size at user.

2) User needs not to contact with PKG during keyupdate, or, PKG is allowed to be offline after sending the revocation list to KU-CSP.

3)Nose cure channel or user authentication is required during key-update between user and KU-CSP. Finally,we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Furthermore, we consider realizing revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure under RDoC model, in which at least one of the KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs collude, it is unable to help such user re-obtain his/her decryptability. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

ACKNOWLEDGMENT

We would like to thank Mangala.C.N, Associate Professor, Department of Computer Science and Engineering, East West institute of technology for her constant support and her guidance and also for providing us the opportunity to contribute on data access through users identity. At last we also thank all faculty members of Department of Computer Science and Engineering for helping us in this work.

REFERENCES

[1].M.Green,S.Hohenberger, and B.Waters, ‖*outsourcing the decryption of ABE ciphertexts*,‖ in proc.20th USENIX Conf. security(SEC11),2011,PP.34-34

[2].Brent waters, –*ciphertext-policy attribute-based encryption* –An expressive,efficient,and provably secure realization. In PKC 53-70, 2011.

[3].Vipul Goyal, Omkat pandey,Amit Sahahi, and Abhishek jain.‖*Bounded ciphertext policy attribute based encryption*‖ in ICALP, 2008, PP 579-591
[4].John Bethencourt. –*Ciphertext-policy attribute based encryption library*‖. From http//acsc.cs.ut exas.edu ,2010.
[5].C. Delerablee, –*identity based broadcast encryption with constant size ciphertexts and private keys*‖ in cryptology-2007,ed springer,pp:200-215
[6].S.Honenberger and B.waters,‖*Attribute based encryption with fast decryption of ABE ciphertext*‖, USENIX, 2011.
[7].S.Yu, C.Wang,K.Ren, W.Lou,‖*Attribute based data sharing with attribute revocation*‖, security(ASIACCS'10),PP.261-270,2010

AUTHORS BIOGRAPHY

Mangala.C.N received the B.E degree in Computer science and Engineering from NCET, Bangalore, VTU in 2006 and got M.Tech degree in Computer Science from RVCE, Bangalore, India. She is currently working as Associate Professor in the faculty of CSE, EWIT- Bangalore, India. Her area of interest includes Image Processing, Data mining, Cloud computing and Big data.

Bhoomika M.U is pursuing her B.E in Computer Science and Engineering in East West institute of Technology, Bangalore, India. His area of interest includes cloud computing and Big Data, Data Mining.

Chandini M is pursuing her B.E in Computer Science and Engineering in East West institute of Technology, Bangalore, India. His area of interest includes Cloud Computing, Big Data and Network Security.

Harshitha R S is pursuing her B.E in Computer Science and Engineering in East West institute of Technology, Bangalore, India. His area of interest includes Cloud Computing, Big Data and Network Security.

Suraj S Gurav is pursuing his B.E in Computer Science and Engineering in East West institute of Technology, Bangalore, India. His area of interest includes Cloud Computing, Big Data,Data Mining.