INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) ISSN: 2349-4689
Volume-25, Number - 03, 2016

Development of Identity-Based Encryption With Added Secret Key for Enhancing the Security of Cloud Computing

Kalpana Chouksey[1], Dr. Vineet Richhariya[2]

[1]*M-Tech Research Scholar,* [2]*HOD & Research Guide*

Department of Computer Science & Engineering Lakshmi Narain College of Technology, Bhopal

Abstract- In Cloud Computing, security is a challenging problem. Usingan Identity-Based Encryption with added secret key enhances the privacy of the users and also provides identity based authentication to the users in an appropriate manner. The principal objective of Identity-Based Encryption with added secret key in cloud computing is to provide privacy to the users to access their data or file stored on the cloud. Advanced Encryption Standard (AES) Algorithm is used to enhance security to the access of the data stored on cloud. The Advanced Encryption Standard (AES) is a symmetric block cipher to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive user data. AES is used for different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information and when used in an NSA approved cryptographic module. The main focus of this research is on security enhancement with added secret key in cloud. This provides user identity based access of data using secret key provided by cloud. Identity of the user can be recognized through his email id provided during his registration. The proposed Identity-Based Encryption with added a secret key in cloud enhances security and also personalizes the user data or file stored on the cloud. And also provide user identity-based access to the data using key provided by the cloud. In this proposed system, Advanced Encryption Standard algorithm is used. Proposed algorithm is implemented in JAVA (Net beans) Experimental results show that the security is enhanced to provide privacy to the preconized data of the user stored or can easily accessed on the cloud.

I. INTRODUCTION

Cloud Computing also known as “on demand computing”, is a kind of Internet based computing, where users can share resources, data and information are provided to computers and other devices on-demand. Cloud Computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers very easily.

Cloud computing now a day has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. The term cloud has been used to refer to platforms for distributed computing. Cloud computing is the result of the evolution and adoption of existing technologies. The goal of cloud computing is to allow users to take benefit from all of these technologies, without any need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users to focus on their core business.

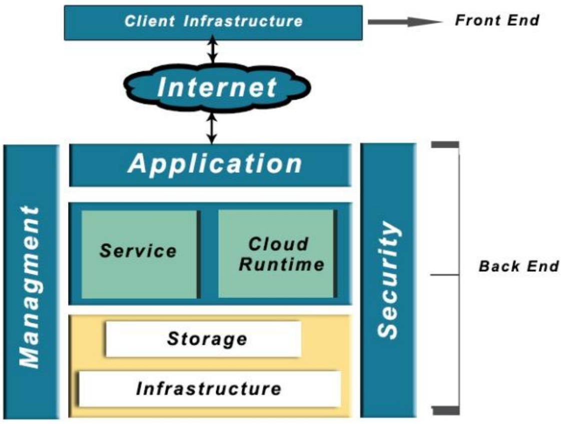


Fig 1. Cloud Computing Architecture

Cloud computing provides all of its resources as services, and makes use of the well-established standards and allow global and easy access to cloud services in a standardized way. Cloud computing is a kind of grid computing and it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing also provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

II. SECURITY ISSUES ASSOCIATED WITH CLOUD

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories:

1. Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected.
2. When an organization decides to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance survey report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees after every data stored and who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity on cloud.
3. In order to conserve resources, reduce the cost and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors) any time from any location. To handle such sensitive situations, cloud service providers should ensure proper data separation and logical storage segregation.

ADVANTAGES OF CLOUD COMPUTING

1. Increases working efficiency on cloud.
2. Helps improve cash flow on business transactions.
3. Provides flexibility in storing data.
4. Disaster recovery is faster and saves time.
5. Automatic software updates including security updates.
6. Capital –expenditure free means reduces the high cost of hardware.
7. Increased collaboration means accessing, editing on data is easy.
8. Work from anywhere on cloud.
9. Document controls means easy accessibility.
10. Data is more secure on cloud.
11. Competitiveness, allows smaller business to act faster.
12. Environmentally friendly.

1.7 APPLICATIONS OF CLOUD COMPUTING

1. Cloud application in ECG data analysis:

Cloud technology is an attractive option for developing health-monitoring systems because of the capillary development of internet connectivity and its accessibility from any device at any time. ECG provides a particular waveform to detect heart diseases.

2. Cloud application in protein structure prediction:

Machine learning techniques are used for the prediction task to determine the secondary structure of proteins. Jeeva is a project that investigates the use of cloud technologies for protein structure prediction.

3. Cloud application in gene-expression data analysis for cancer diagnosis:

Gene-expression profiling is utilized to understand the biological processes that are triggered by the treatment of a cellular level. Cancer diagnosis and treatment is another application of gene-expression profiling.

4. Cloud application in satellite image processing:

Satellite remote sensing produces hundreds of giga bytes of raw images that are processed to become the basis of a number of different GIS(Geographic Information System) products. The suitable infrastructure is provided by cloud computing to support such application scenario.

5. Cloud application in social networking application:

A completely customized stack of open source technologies modified and refined forms the back end of the largest social network. For developing cloud applications, these technologies form a powerful platform. This platform mainly helps Facebook itself and provides APIs to combine third-party applications with Facebook's coreinfrastructure to provide extra services like social games and quizzes generation.

III. PROPOSED METHODOLOGY

METHODOLOGY:

In proposed methodology, mainly focused on security enhancement using Identity-Based Encryption with added a secret key, in order to provide privacy in accessing the user data stored on cloud. In this proposed system, work and improvement done in two areas:

- Security Enhancement:

In security enhancement, Random Encryption Key is generated to provide privacy in accessing user stored data on cloud. Another thing is that it is identity- based encryption that means only a particular user can access his/her stored on cloud using cloud provided private key. Through a verification send on the registered email-id, then only user can store and access his data on cloud.

- Encryption Algorithm:

In based paper, AES(Attribute Based Encryption) algorithm is used but in the proposed system, AES(Advanced Encryption Standard) algorithm is used to enhance the security on cloud.

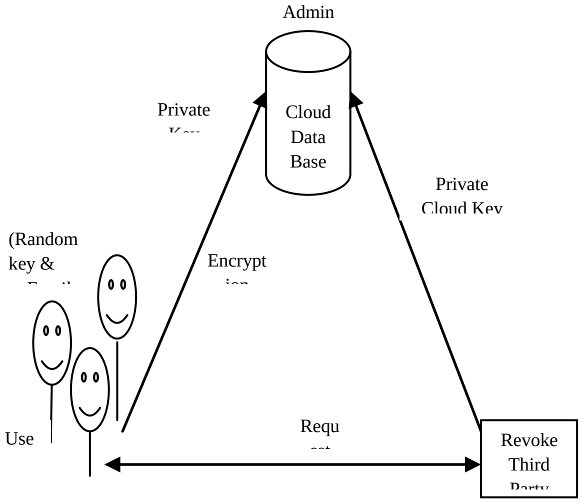
Proposed Algorithm:

The Advanced Encryption Standard (AES), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute Of Standards and Technology (NIST) in 2001.

AES is based on a design principle called as a substitution-permutation networkcombination of both substitution and permutation, and is fast in both software and hardware.Unlike its predecessor DES, AES does not use a Feistel Network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By the contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and maximum of 256 bits.

AES operates on a 4 × 4 column-major order matrix of bytes, termed as the state although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

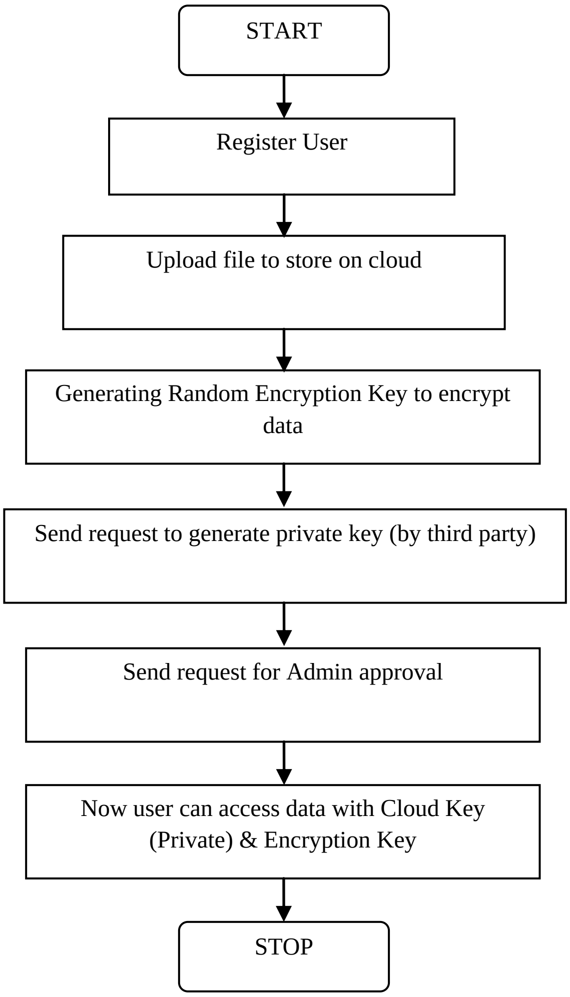
PROPOSED BLOCK DIAGRAM:



PROPOSED FLOW DIAGRAM:

PROPOSED SET OF OPERATION:

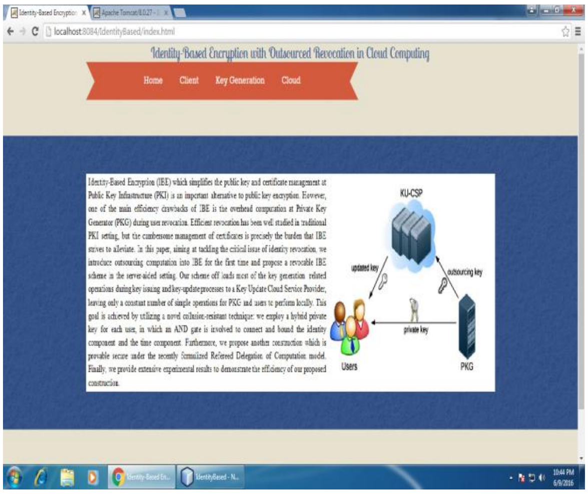
1. *Initially click on client on home page.*
2. *Firstly user register himself on cloud.*
3. *Login using registered username.*
4. *Upload the file or to be stored on cloud.*
5. *Give file name and note file no. and key.*
6. *Click on upload.*
7. *To view data click above on database and logout.*
8. *Send request for key.*
9. *Login to pkg for key (username Pkg and password pkg).*
10. *Scroll down and select username then click on key generation.*
11. *Go to home page and click on key generation.*
12. *Now login using Admin id and password admin.*
13. *Select username and file name from Admin Key Generation.*


START
Register User
Upload file to store on cloud
Generating Random Encryption Key to encrypt data
Send request to generate private key (by third party)
Send request for Admin approval
Now user can access data with Cloud Key (Private) & Encryption Key
STOP

IV. MPLEMENTATATION RESULTS:

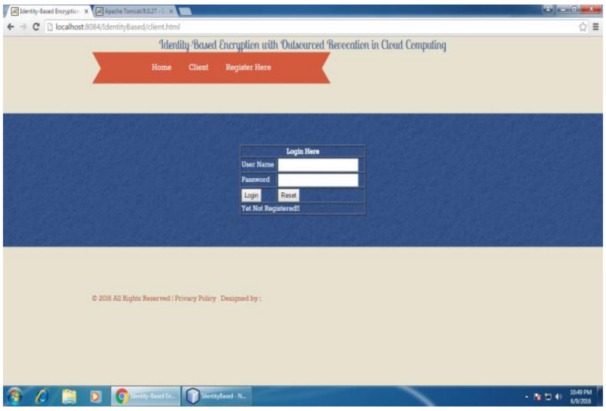
14. *Enter Encrypted Key.*
15. *Then click on send key.*
16. *Go to home page and click on Cloud.*
17. *Login using registered username and password.*
18. *Click on View Keys.*
19. *Note down the cloud key.*
20. *Click below to view original data.*
21. *Enter filename and Cloud Key then click on Verify.*
22. *Enter Encryption Key to view the saved data.*
23. *Logout.*

Step: 1 initially open home page.


localhost:8084/IdentityBased/index.html
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
Client
Key Generation
Cloud
KU-CSP
updated key
outsourcing key
private key
Users
PKG
10:44 PM
6/9/2016

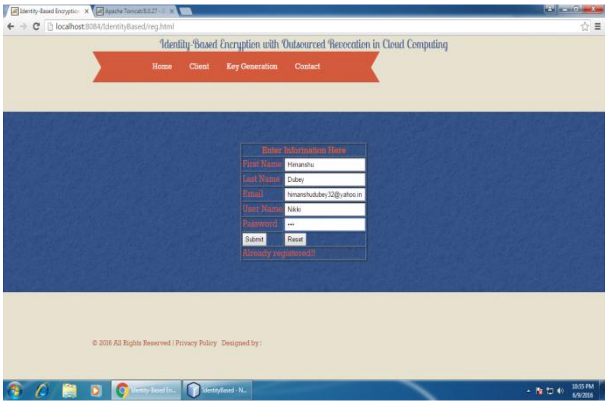
Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme off loads most of the key generation related operations during key issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users 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, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Step:2 Click on the "Client".


localhost:8084/IdentityBased/client.html
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
Client
Register Here
Login Here
User Name
Password
Login
Reset
Yet Not Registered!!
© 2016 All Rights Reserved | Privacy Policy Designed by :
10:49 PM
6/9/2016

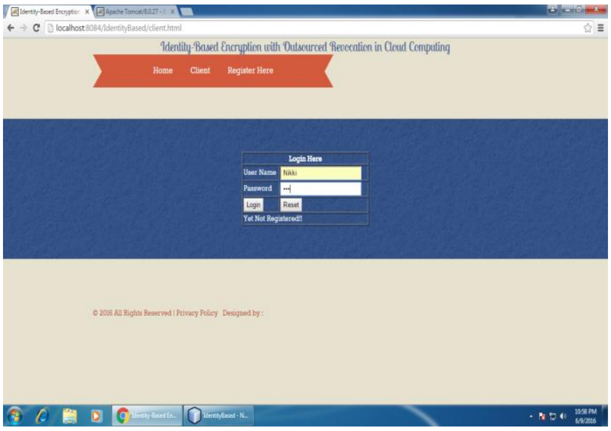
Step: 3Click on "Register Here"

New users register by username id and password and fill all correct details like email id asked. Then click on "Submit".


localhost:8084/IdentityBased/reg.html
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
Client
Key Generation
Contact
Enter Information Here
Submit
Reset
Already registered!!
© 2016 All Rights Reserved | Privacy Policy Designed by :
10:55 PM
6/9/2016

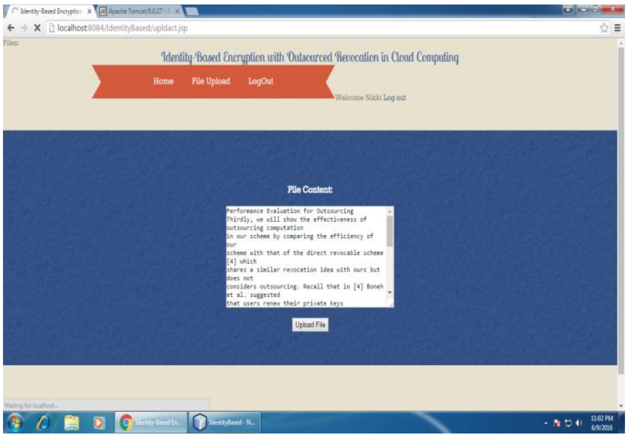
First Name: Himanshu
Last Name: Dubey
Email: himanshudubey32@yahoo.in
User Name: Nikki
Password: •••

Step: 4 Login using Username and password. Then click on "Login".


localhost:8084/IdentityBased/client.html
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
Client
Register Here
Login Here
Login
Reset
Yet Not Registered!!
© 2016 All Rights Reserved | Privacy Policy Designed by :
10:58 PM
6/9/2016

User Name: Nikki
Password: •••

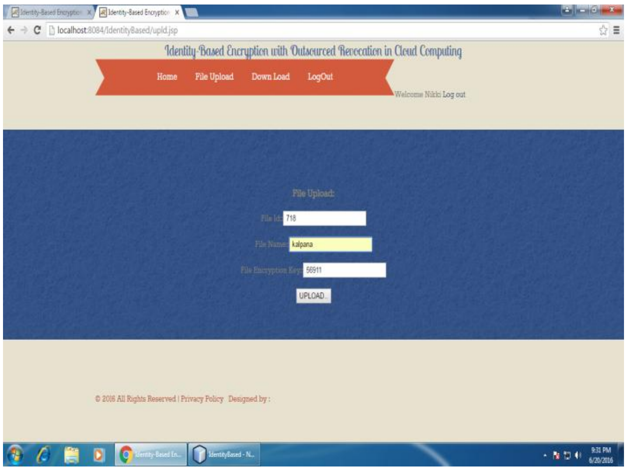
Step: 5 Choose a file user want to store on cloud. Then click on "Upload File" and logout from user id.


localhost:8084/IdentityBased/upldact.jsp
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
File Upload
LogOut
Welcome Nikki Log out
Upload File
11:02 PM
6/9/2016

File Content:

```
Performance Evaluation for Outsourcing
Thirdly, we will show the effectiveness of
outsourcing computation
in our scheme by comparing the efficiency of
our
scheme with that of the direct revocable scheme
[4] which
shares a similar revocation idea with ours but
does not
considers outsourcing. Recall that in [4] Boneh
et al. suggested
that users renew their private keys
```

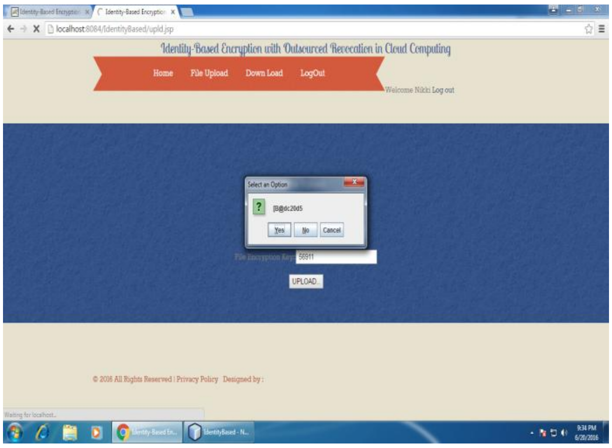
Step: 6 Click "ok" on the dialog box. Then give file name and key. Click on upload.


localhost:8084/IdentityBased/upld.jsp
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
File Upload
Down Load
LogOut
Welcome Nikki Log out
UPLOAD..
© 2016 All Rights Reserved | Privacy Policy Designed by :
9:31 PM
6/20/2016

File Upload:

File Id:: 718
File Name:: kalpana
File Encryption Key:: 56911

Step:7 Then a check box comes click "yes".



localhost:8084/IdentityBased/upld.jsp

Identity-Based Encryption with Outsourced Revocation in Cloud Computing

Home File Upload Down Load LogOut

Welcome Nikki Log out

Select an Option

[B@dc20d5

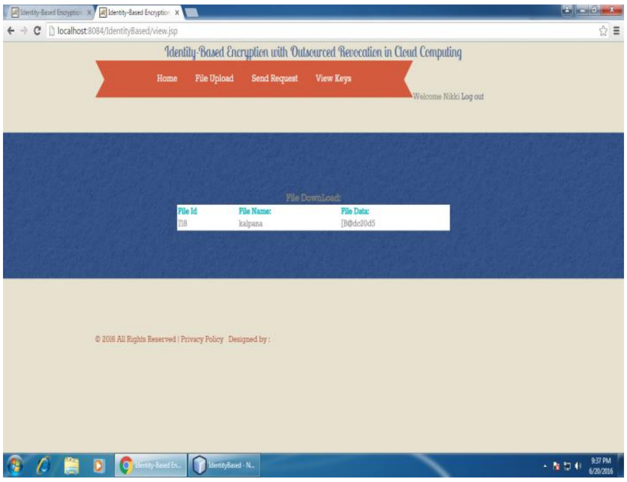
Yes No Cancel

File Encryption Key: 56911

UPLOAD

© 2016 All Rights Reserved | Privacy Policy Designed by :

Step: 8 To view upload data , Go to view database.



localhost:8084/IdentityBased/view.jsp

Identity-Based Encryption with Outsourced Revocation in Cloud Computing

Home File Upload Send Request View Keys

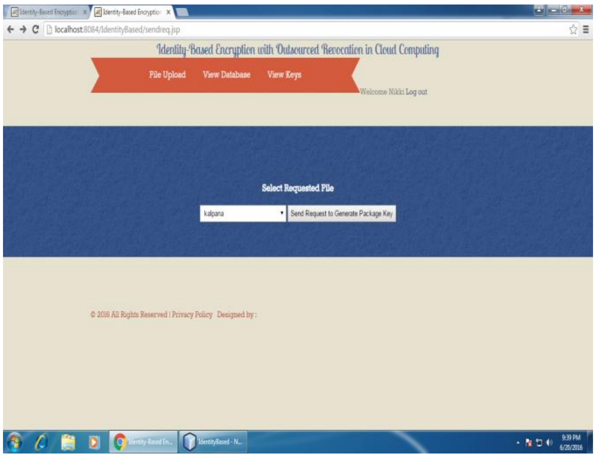
Welcome Nikki Log out

File DownLoad:

File Id	File Name:	File Data:
718	kalpana	[B@dc20d5

© 2016 All Rights Reserved | Privacy Policy Designed by :

Step: 9 Now click on "Send Key Request". Select requested file and send request to Generate Package Key and Logout.



localhost:8084/IdentityBased/sendreq.jsp

Identity-Based Encryption with Outsourced Revocation in Cloud Computing

File Upload View Database View Keys

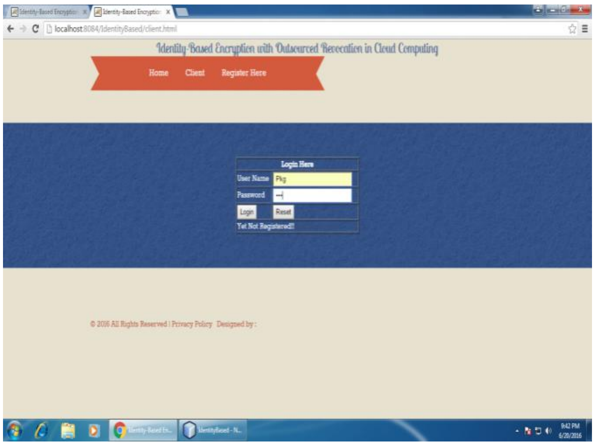
Welcome Nikki Log out

Select Requested File

kalpana ▾ Send Request to Generate Package Key

© 2016 All Rights Reserved | Privacy Policy Designed by :

Step: 10Go toclientthen login using Pkg id and pkg password.



localhost:8084/IdentityBased/client.html

Identity-Based Encryption with Outsourced Revocation in Cloud Computing

Home Client Register Here

Login Here

User Name: Pkg

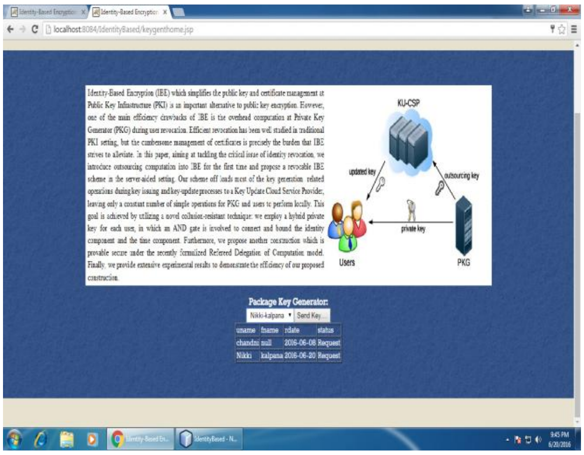
Password: ---

Login Reset

Yet Not Registered!!

© 2016 All Rights Reserved | Privacy Policy Designed by :

Step:11 Scroll down and select username, then click on send key.



localhost:8084/IdentityBased/keygenthome.jsp

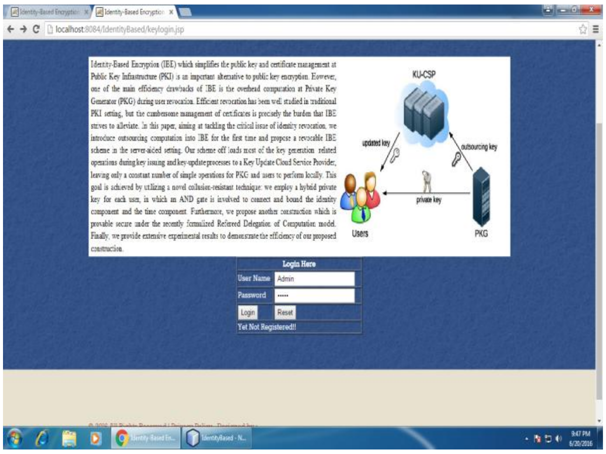
Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme off loads most of the key generation related operations during key issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users 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, we propose another construction which is provable secure under the recently formalized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Package Key Generator:

Nikki-kalpana ▾ Send Key...

uname	fname	rdate	status
chandni	null	2016-06-08	Request
Nikki	kalpana	2016-06-20	Request

Step:12 Go to home page and click on "Key Generation". Now login using Admin id and admin password.



localhost:8084/IdentityBased/keylogin.jsp

Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme off loads most of the key generation related operations during key issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users 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, we propose another construction which is provable secure under the recently formalized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Login Here

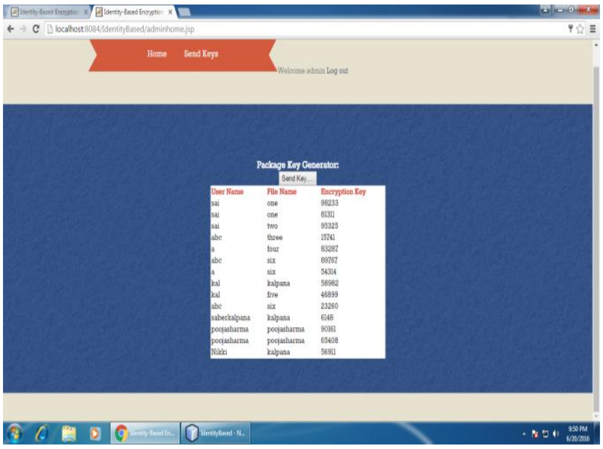
User Name: Admin

Password: -----

Login Reset

Yet Not Registered!!

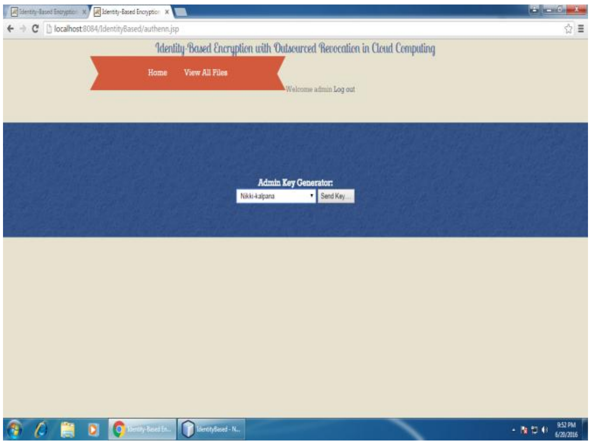
Step: 13 Click on "Send Key" below Package Key Generator. Note down the Encryption Key.



Package Key Generator:

User Name	File Name	Encryption Key
sai	one	98233
sai	one	81311
sai	two	95325
abc	three	15741
a	four	83287
abc	six	89767
a	six	54314
kal	kalpana	58982
kal	five	46899
abc	six	23260
saberkalpana	kalpana	6148
poojasharma	poojasharma	90161
poojasharma	poojasharma	65408
Nikki	kalpana	56911

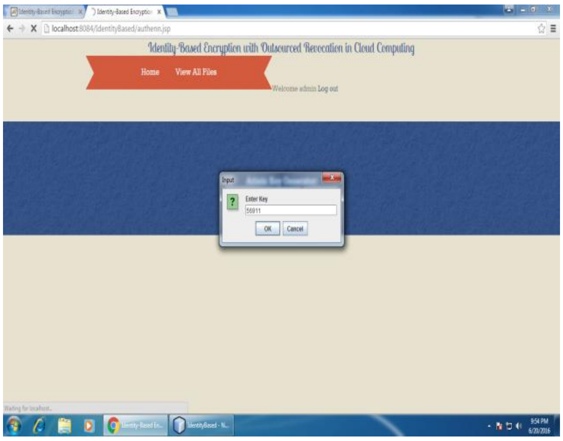
Step: 14 Below Admin Key Generator select username with filename and click on "Send Key".


localhost:8084/IdentityBased/authenn.jsp
Identity Based Encryption with Outsourced Revocation in Cloud Computing
Home
View All Files
Welcome admin Log out
Send Key....

Admin Key Generator:

Nikki-kalpana

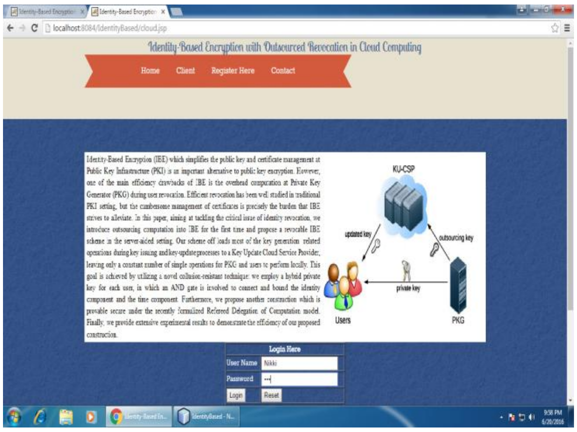
Step:15Enter the Encryption Key, click on "ok" and Logout.


localhost:8084/IdentityBased/authenn.jsp
Identity Based Encryption with Outsourced Revocation in Cloud Computing
Home
View All Files
Welcome admin Log out
Input
OK
Cancel

Enter Key

56911

Step:16 Go to Cloud. Login using username.


localhost:8084/IdentityBased/cloud.jsp
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
Client
Register Here
Contact
KU-CSP
updated key
outsourcing key
private key
Users
PKG
Login
Reset

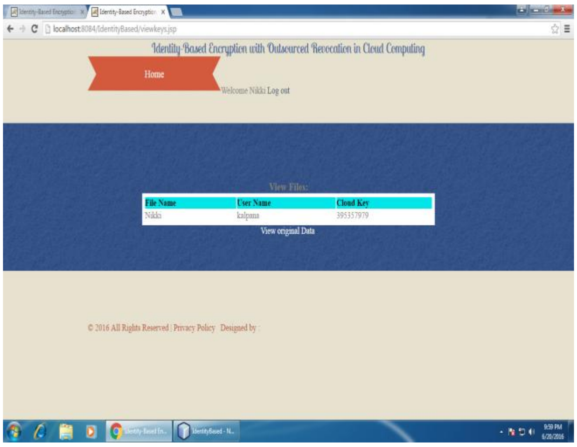
Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme off loads most of the key generation related operations during key issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users 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, we propose another construction which is provable secure under the recently formalized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Login Here

User Name: Nikki

Password: •••

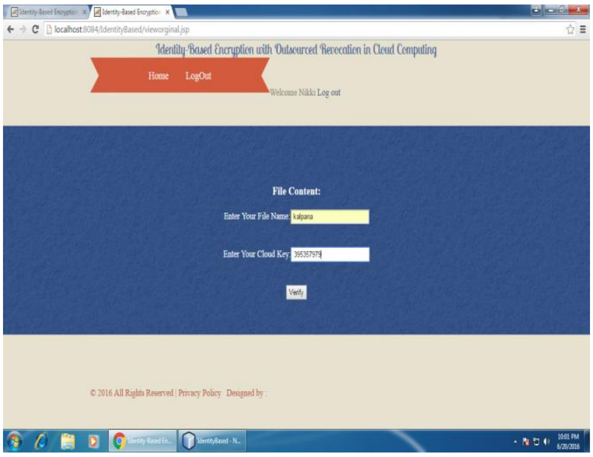
Step:17 Click on "view keys". Note down the cloud key.


localhost:8084/IdentityBased/viewkeys.jsp
Identity Based Encryption with Outsourced Revocation in Cloud Computing
Home
Welcome Nikki Log out
View original Data
© 2016 All Rights Reserved | Privacy Policy Designed by :

View Files:

File Name	User Name	Cloud Key
Nikki	kalpana	395357979

Step: 18 Now click below on "view original data". Enter file name and cloud key. Then click on "verify".

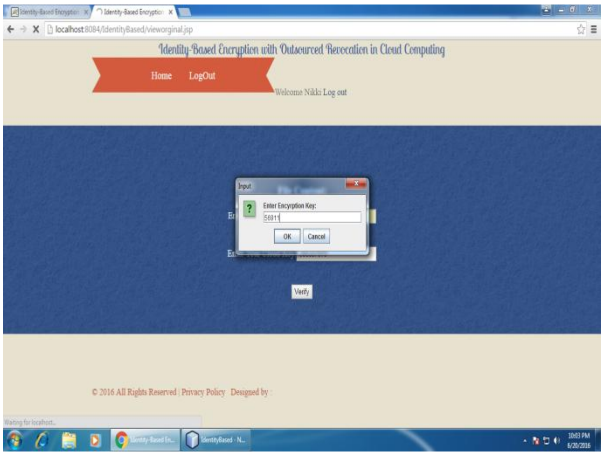

localhost:8084/IdentityBased/vieworginal.jsp
Identity Based Encryption with Outsourced Revocation in Cloud Computing
Home
LogOut
Welcome Nikki Log out
Verify
© 2016 All Rights Reserved | Privacy Policy Designed by :

File Content:

Enter Your File Name: kalpana

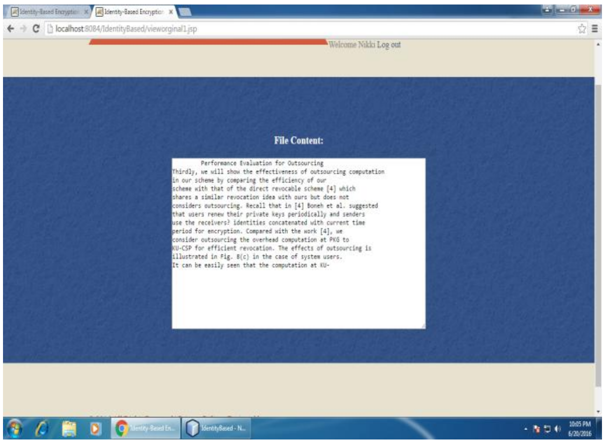
Enter Your Cloud Key: 395357979

Step: 19 Now enter Encryption Key and click on "ok".


Identity-Based Encryption
Identity-Based Encryption
localhost:8084/IdentityBased/vieworginal.jsp
Identity-Based Encryption with Outsourced Revocation in Cloud Computing
Home
LogOut
Welcome Nikki Log out
Input
OK
Cancel
Verify
© 2016 All Rights Reserved | Privacy Policy Designed by
Waiting for localhost...
Identity-Based En...
IdentityBased - N...
10:03 PM
6/20/2016

Enter Encryption Key: 56911

Step: 20 As a result file content is visible and Logout.


Identity-Based Encryption
Identity-Based Encryption
localhost:8084/IdentityBased/vieworginal1.jsp
Welcome Nikki Log out
Identity-Based En...
IdentityBased - N...
10:05 PM
6/20/2016

File Content:

```
        Performance Evaluation for Outsourcing
Thirdly, we will show the effectiveness of outsourcing computation
in our scheme by comparing the efficiency of our
scheme with that of the direct revocable scheme [4] which
shares a similar revocation idea with ours but does not
considers outsourcing. Recall that in [4] Boneh et al. suggested
that users renew their private keys periodically and senders
use the receivers? identities concatenated with current time
period for encryption. Compared with the work [4], we
consider outsourcing the overhead computation at PKG to
KU-CSP for efficient revocation. The effects of outsourcing is
illustrated in Fig. 8(c) in the case of system users.
It can be easily seen that the computation at KU-
```

Table 1: System Parameter Comparison

Parameters	Existing System	Proposed System
Security Levels	Three Level Security	Four Level Security
Private Key Generation	Using Random Key Only	Using Random Key + Using Email ID
Encryption Technique	Attribute Based Encryption (ABE)	Advanced Encryption Standard (AES)
Package Key Generation	Third Party	Third Party
Database	Cloud	Cloud
User Authentication	Administrator	Administrator

V. CONCLUSION AND FUTURE WORK

Using Identity-Based Encryption with added a secret private key , user store their data or file on cloud using cloud key and can only particular user can access that data or file from cloud by registering initially on cloud. This enhances the security to the user data or file stored on cloud and also increase the attackers time while trying to steal the information. This also provided privacy to the users for storing their confidential file on cloud and using cloud key user can access the file. In this dissertation, levels of security are increased.

In keeping mind all the parameters, in future we can further improve this system by applying new techniques in order to enhance more security. Some another algorithms can be used to provide more accuracy and security to the system.

REFERENCES:

[1] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, Senior Member, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing" IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 2, FEBRUARY 2015.

[2] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In Shoup [107], pages 205{222.

[3] Michel Abdalla, Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Robust public-key and identity-based encryption. Unpublished manuscript, 2008.

[4] Michel Abdalla, Mihir Bellare, and Gregory Neven. A provable-security treatment of robust encryption. Cryptology ePrint Archive, Report 2008/440, 2008. http://eprint.iacr.org/.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput. Commun. Security (CCS'08), 2008, pp. 417–426.

[6] Shane Balfe, Kent D. Boklan, Zev Klagsbrun, and Kenneth G. Paterson. Key refreshing in identity-based cryptography and its applications in MANETs. IEEE Military Communications Conference, MILCOM, 2007.

[7] Manuel Barbosa and Pooya Farshim. E_cient identity-based key encapsulation

to multiple parties. In Smart [109], pages 428{441.

[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Annu. ACM Symp. Theory Comput. (STOC'97), 1997, pp. 506–516.

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography (TCC'05), 2005, pp. 264–282.

[10] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegationof computation," in Information Theoretic Security, A. Smith, Ed.Berlin, Germany: Springer, 2012, vol. 7412, pp. 37–61.

[11] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secureoutsourcing algorithms of modular exponentiations," in Proc. 17thEur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.

[12] M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebracomputations," in Proc. 5th ACM Symp. Inf. Comput. Commun.Security (ASIACCS'10), 2010, pp. 48–59.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes,"in Advances in Cryptology (CRYPTO), G. Blakley and D. Chaum, Eds.Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.

[14] C. Cocks, "An identity based encryption scheme based on quadraticresidues," in Cryptography and Coding, B. Honary, Ed. Berlin/Heidelberg: Springer, 2001, vol. 2260, pp. 360–363.

[15] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-keyencryption scheme," in Advances in Cryptology (EUROCRYPT'03),E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656,pp. 646–646.

[16] D. Boneh and X. Boyen, "Efficient selective-id secure identity-basedencryption without random oracles," in Advances in Cryptology(EUROCRYPT'04), C. Cachin and J. Camenisch, Eds. Berlin,Germany: Springer, 2004, vol. 3027, pp. 223–238.

[17] D. Boneh and X. Boyen, "Secure identity based encryption withoutrandom oracles," in Advances in Cryptology (CRYPTO'04),M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152,pp. 197–206.

[18] B. Waters, "Efficient identity-based encryption without randomoracles," in Advances in Cryptology (EUROCRYPT'05), R. Cramer,Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.

[19] C. Gentry, "Practical identity-based encryption without randomoracles," in Advances in Cryptology (EUROCRYPT'06), S. Vaudenay,Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[20] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hardlattices and new cryptographic constructions," in Proc. 40th Annu.ACM Symp. Theory Comput. (STOC'08), 2008, pp. 197–206.

[21] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe inthe standard model," in Advances in Cryptology (EUROCRYPT'10),H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110,pp. 553–572.

[22] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or howto delegate a lattice basis," in Advances in Cryptology (EUROCRYPT'10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010,vol. 6110, pp. 523–552.