IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 9, September 2017

Secured Data Sharing System using High Level Cryptography

Ch. Sravanthi[1], Mahesh Vasupalli[2], Mr. Y. Ramesh Kumar[3]

PG Scholar, Dept of C.S.E., Avanthi College of Engineering, Visakhapatnam, India[1]

Assistant Professor, Dept of C.S.E., Avanthi College of Engineering, Visakhapatnam, India[2]

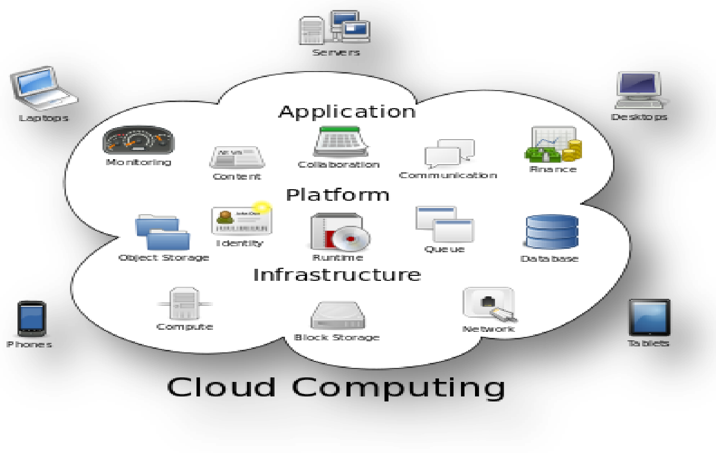
Professor, Dept of C.S.E., Avanthi College of Engineering, Visakhapatnam, India[3]

Abstract: Cloud computing is most Prominent Solution for large data storage and data sharing, which has lot of benefits for industry and individuals. However, there exists a natural problem for directly outsource and share the data in the cloud server since the they contain valuable information so it requires the high-level security. It is necessary to provide the highly cryptographically access control Mechanism for data sharing. Therefore, in this project we use Identity-based encryption, which is a promising cryptography technique for building a practical data sharing system. Since access, control is not a static mechanism. When some user's authorization is expired, there should be a mechanism that can remove him/her from the system. In addition, we need to check the revoked user cannot access both the previously and subsequently shared data. So has to make this system to be implement we propose revocable-storage identity-based encryption, which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. The proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

Keywords: Revocation, Encryption, Key Exchange, Private key generator, cipher text.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). An end user layer that encapsulates the end user perspective on cloud services completes the three service models or layers. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

DOI10.17148/IJARCCE.2017.6933

II. EXISTING SYSTEM

Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority. Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. However, this scheme only achieves selective security. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme, Chen et al. constructed a RIBE scheme from lattices.

III. PROPOSED SYSTEM

In the proposed system , we used a concept called revocable-storage identity-based encryption (RSIBE) for building a cost-effective data sharing system that fulfills the three security goals decryption, and it is inadvisable to update the cipher text periodically by using secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re-encrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her. The proposed system attains the following characteristics:

- **We prove that the security of the proposed**
- **We can provide formal definitions for RS-IBE and its corresponding security model; and backward/forward secrecy simultaneously**
- The security goals are:
- **Data confidentiality**: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.
- **Backward secrecy**: Backward secrecy says that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequentlyshared data that are still encrypted under his/her identity.
- **Forward secrecy**: Forward secrecy means that, when a user's authority is expired, or a user's secret scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption.
- □In addition to security, this system will reduce the time complexity and provide a better performance.

IV.1 PRELIMINARIES

DECISIONAL ℓ-BDHE ASSUMPTION:

The decisional ℓ-BDHE problem is formalized as follows. Choose a group $G_1$with prime order p according to the security parameter. Select a generator g of G1 and a, s<-R ZP and let fi=g ai..T Provide the vector f= (g, g^s, f_1, ..., f_ℓ, $f_{\ell+2}$, ..., $f_{2\ell}$) and an element D∈G_2 to a probabilistic polynomial-time) algorithm C, it outputs 0 to indicate that D = e(g^s, $g^{a\ell+1}$), and outputs 1 to indicate that D is a random element from G_2.

DEFINITION IN RS-IBE:

A revocable-storage identity-based encryption scheme with message space **M**, identity space **I** and total number of time periods T is comprised of the following seven polynomial time algorithms

1.setup(1^λ, T, N): the setup algorithm takes as input the security parameter λ ,the time bound T and the maximum number of system users N , and it outputs the public parameter P P and the master secret key M SK, associated with the initial revocation list RL=∅ and state st.

2. PKGen(P P, M SK, ID): The private key generation algorithm takes as input P P , M SK and an identity ID ∈**I**, and it generates a private key $SK_{ID}$for ID and an updated state st.

3. KeyUpdate(P P, M SK, RL, t, st): The key update algorithm takes as input P P , M SK, the current revocation list RL, the key update time t≤T and the state st, it outputs the key update KU_t.

4.DKGen (P P, SK_{ID}, KU_t): The decryption key generation algorithm takes as input P P , SK_{ID} and KUwith time period t, and it generates a decryption key t or a symbol ⊥ to illustrate that DKID,t for IDID has been previously revoked.

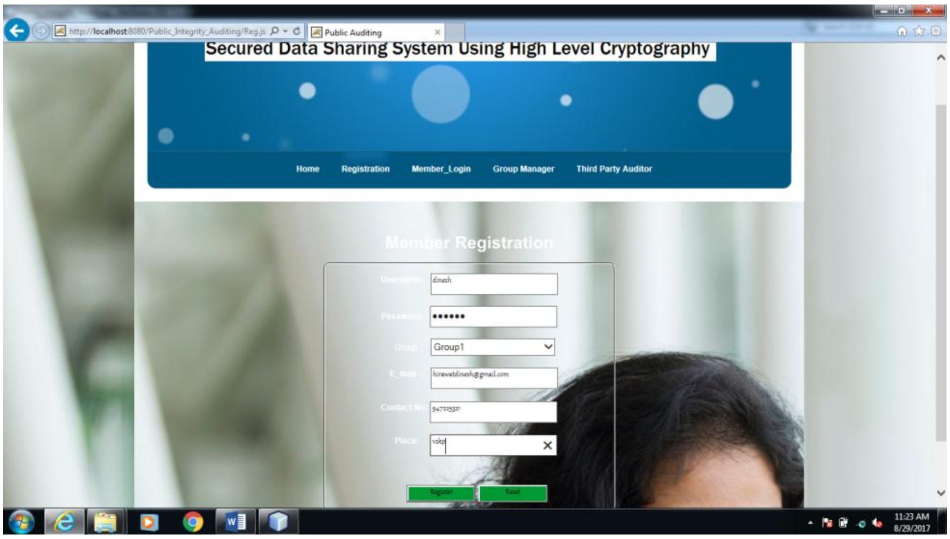
5. Encrypt (P P, ID, t, M): The encryption algorithm takesas input P P , an identity ID, a time period t≤T , and a message M∈**M** to be encrypted, and outputs a cipher text $CT_{ID,t}$.
6. CT Update(P P, $CT_{ID,t}$, t'): The cipher text update algorithm takes as input P P , $CT_{ID,t}$ and a new time period $t' \geq t$, and it outputs an updated ciphertext$CT_{ID,t'}$.
7. Decrypt(P P, $CT_{ID,t}$, $DK_{ID,t'}$): The decryption algorithm takes as input P P , $CT_{ID,t}$, $DK_{ID,t'}$, and it recovers the encrypted message M or a distinguished symbol ⊥ indicating that $CT_{ID,t}$ is an invalid cipher text.
8. Revoke (P P, ID, RL, t, st): The revocation algorithmtakes as input P P , an identity ID∈**I** to be revoked, the current revocation list RL, a state st and revocation time period t≤T , and it updates RL to a new one.

ADVANTAGES OF PROPOSED SYSTEM

The common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints.

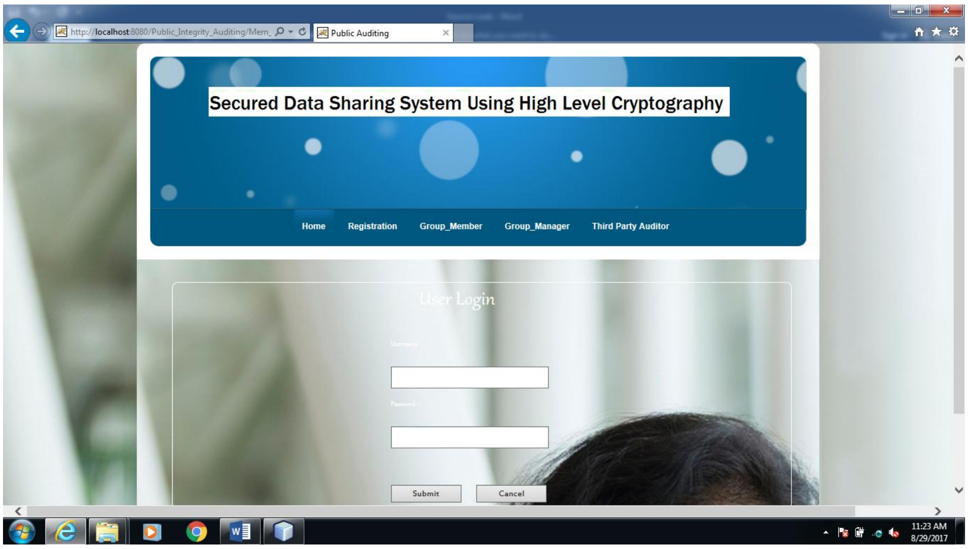
- **Data confidentiality**: Unauthorized users should be prevented from accessing the pla
- **Backward secrecy**: Backward secrecy says that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity. In text of the shared data stored in the cloud server.
- **Forward secrecy**: Forward secrecy means that, when a user's authority is expired, or a user's secret scheme in the standard model, In addition to security, this system will reduce the time complexity and provide a better performance.

V. EXPERIMENTAL RESULTS


http://localhost:8080/Public_Integrity_Auditing/Reg.js
Public Auditing
Secured Data Sharing System Using High Level Cryptography
Home
Registration
Member_Login
Group Manager
Third Party Auditor
Register
Reset
11:23 AM
8/29/2017

Member Registration

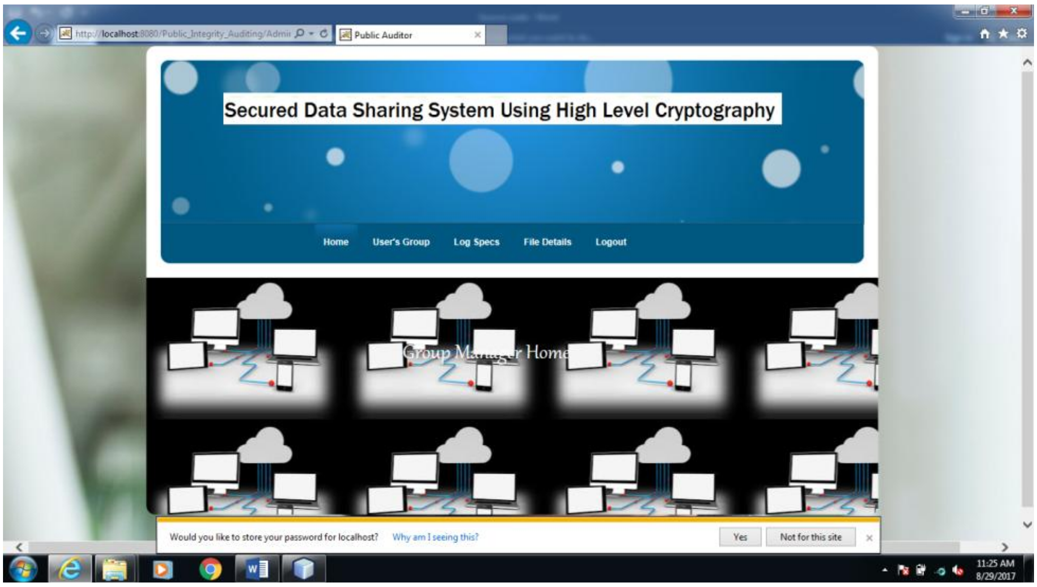
Username: dinesh
Password: ••••••
Group: Group1
E_mail: kirawatdinesh@gmail.com
Contact No: 94775537
Place: vskp


http://localhost:8080/Public_Integrity_Auditing/Mem_
Public Auditing
Secured Data Sharing System Using High Level Cryptography
Home
Registration
Group_Member
Group_Manager
Third Party Auditor
Submit
Cancel
11:23 AM
8/29/2017

User Login

Username
Password :

DOI10.17148/IJARCCE.2017.6933



Would you like to store your password for localhost? Why am I seeing this?

VI. CONCLUSION

Focusing on the 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 key update, in other words, PKG is allowed to be offline 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. Furthermore, we consider realizing revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure underRDoCmodel, in which at least one of the KU-CSPs is assumed 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, For future enhancement, the proposed system can be extended by implementing another protocol, which is more secured, efficient, and feasible when compared to the DL- based protocol. Another alternative is the IF-(Integer Factoring) based protocol whose security depends on the combination of RSA Signature and One-way-hash function. The protocol provides deniable authentication and protects privacy of the digital certificate. In this project, we have used AES algorithm for secure exchange of data between the entities for further extension our approach can be applied to more advanced and secured cryptographic techniques for secure exchange of data.

REFERENCES

[1] Network Working Group, ―Internet X.509 public key infrastructure certificate andcrl profile, RFC: 2459," Jan. 1999.
[2] C. Tang and D. Wu, ―An efficient mobile authentication scheme for wireless networks," IEEE Trans. Wireless Commun., vol. 7, pp. 1408-1416, Apr. 2008.
[3] G. Yang, Q. Huang, D. Wong, and X. Deng, ―An efficient mobile authentication scheme for wireless networks," IEEE Trans. Wireless Commun., vol. 9, pp. 168-174, Jan. 2010.
[4] J. Chun, J. Hwang, and D. Lee, ―A note on leakage-resilient authenticated key exchange," IEEE Trans. Wireless Commun., vol. 8, pp. 2274-2279, May 2009.
[5] D. Chaum and H. van Antwerpen, ―Undeniable signatures," Advances in Cryptology - Crypto'89, Lecture Notes in Computer Science, vol. 435, pp. 212-217, 1989.
[6] M. Bohøj and M. Kjeldsen, ―Cryptography report: undeniable signature schemes,"Tech. Rep., Dec. 15, 2006.
[7] X. Huang, Y. Mu, W. Susilo, and W. Wu, ―Provably secure pairing-based convertible undeniable signature with short signature length," Pairing-Based Cryptography - C Pairing 2007, vol. 4575/2007 of Lecture Notes in Computer Science, pp. 367-391, Springer Berlin / Heidelberg, 2007.
[8] M. Jakobsson, K. Sako, and R. Impagliazzo, ―Designated verifier proofs and theirapplications," Advances in Cryptology - EUROCRYPT, pp. 143-154, 1996. LNCS Vol 1070. [9] D. Chaum, ―Private signature and proof systems," 1996.
[9] R. Rivest, A. Shamir, and Y. Tauman, ―How to leak a secret," Advances inCryptology-ASIACRYPT, Lecture Notes in Computer Science, vol. 2248/2001, Springer Berlin / Heidelberg, 2001.
[10] J. Ren and L. Harn, ―Generalized ring signatures," IEEE Trans. Dependable Secure Comput., vol. 5, no. 4, Oct.-Dec., pp. 155-163, 2008.
[11] S. Saeednia, S. Kremer, and O. Markowitch, ―An efficient strong designated verifier signature scheme," ICISC 2003, vol. 2836 of Springer Lecture Notes in Computer Science, pp. 40-54, 2003.

DOI10.17148/IJARCCE.2017.6933

BIOGRAPHIES

Chipurapalli Sravanthi is a PG scholar in computer science and engineering Department, Avanthi College Of Engineering Bhogapuram, Visakhapatnam, India. She received his Bachelor degree in 2013. Her research interests are image Processing, computer Networks, Algorithms. Etc..

Mr. Mahesh Vasupalli is a Assistant Professor in computer science and engineering Department, Avanthi Institute Of Engineering & Technology, Bhogapuram, Visakhapatnam, India. His research interests are image processing, Computer Networks, Data Mining.

Mr. Y. Ramesh Kumar is a Professor in computer science and engineering Department, Avanthi Institute Of Engineering & Technology, Bhogapuram, Visakhapatnam, India. His research interests are image processing, Computer Networks, Data.

DOI10.17148/IJARCCE.2017.6933