International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Identity-Based Encryption with Cloud Revocation Authority and Its Applications

Mrs. Shravani[1] Manpreet Kour[2] M. Nikhitha[3] M. Ram Charan[4]

Associate Professor, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India[1]
B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[2]
B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[3]
B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[4]

ABSTRACT;- *In this paper we study regarding information sharing has never been easier with the advances of cloud computing, because of the absence of PKI, the revocation drawback could be a critical issue in IBE settings. Identity-based encryption (IBE) could be a public key cryptosystem. We want to disregards the difficulties to induce public key infrastructure (PKI) and certificate administration in standard public key settings. Many revocable IBE schemes are planned relating to this issue. Recently solve this drawback exploitation embedding Associate in nursing outsourcing computation technique into Identity-based encryption. Our planned system straightforward to recover the IBE theme with a key-update cloud service supplier (KU-CSP). However, their scheme has two shortcomings. One is lack of scalability within the sense that the KU-CSP should keep a secret worth for every user. The opposite defect could be a computation and communication prices area unit more than previous revocable IBE schemes. Within the article, we tend to propose a replacement revocable IBE theme with a cloud revocation authority (CRA) to unravel the two shortcomings, For security analysis, we have a tendency to demonstrate that the planned scheme is semantically secure below the decisional linear Diffie-Hellman (DBDH) assumption. Namely, the performance is considerably improved and also the CRA holds solely a system secret for all the users. Finally, we extend the planned revocable IBE scheme to gift a CRA-aided authentication scheme with period-limited privileges for managing an outsized range of varied cloud services*

1. INTRODUCTION

The cloud provides data storage and sharing services; people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the Cloud, every user in the group is able to not only access and modify shared data. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised. Objective of the project is a revocable IBE scheme with a key-update cloud service provider (KU-CSP). However, their scheme has two shortcomings.

EXISTING SYSTEM

In existing system each user's private key size is 3log *n* points in an elliptic curve, where *n* is the number of leaf nodes (users) in the binary tree. The scheme also results in enormous computation workload for Encryption and decryption procedures. It is enormous load for PKG to maintain the binary tree with a large amount of users.

PROPOSED SYSTEM

In proposed system a new revocable IBE scheme by using multi linear maps, but the size of the public parameters is dependent to the number of users. For achieving constant the size of the public parameters, The concept of revocable IBE scheme to propose the first revocable HIBE scheme. Each user generates a secret key by multiplying some of the partial keys, which depends on the partial keys used by ancestors in the hierarchy tree

2. PROJECT DESCRIPTION

We analyze the problem of detecting misbehaviors based on the system performances we should avoid by using fair share detector.

PROBLEM DEFINITION

Problem Definition in this system each user's private key size is 3log *n* points in an elliptic curve, where *n* is the number of leaf nodes (users) in the binary tree. The scheme also results in enormous computation workload for Encryption and decryption procedures. It is enormous load for PKG to maintain the binary tree with a large amount of users.

METHODOLOGIES

Methodologies are the process of analyzing the principles or procedure for Auditing process in shared data in public cloud with efficient user revocation.

MODULES

- Authentication
- Group Manager
- Store the data into Cloud
- Access Control List
- Maintain Revoke List
- Third Public Auditor

MODULE DESCRIPTION

Authentication

In this module User want to register the personal details in the database and get the authentication processes to go forward. In this module User want to give the database to admin all the registration process is done by an admin. After the registration process completed User can get the authentication permission, by using username and password login website. If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.

Group Manager

In this module the authorized user pay for the cloud server and get the allocation space. And the Authorized person store secures data to cloud. Get the access control and then provide the group members.

Store the data into Cloud

In this module the authorized person store data into cloud that the data will be access the registration user only

Maintain Revocation List

The cloud storage gets the resignation user details from the company and maintains the revocation list. Because identify the unauthorized users and they cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

Maintain Access Control List

The cloud storage gets the registration user details from the company and maintains the revocation list. Because identify who are the authorized users and who can access the cloud resource at any time.

New User

In this module user will register and get the access control key from the managers, so they are access the cloud directly.

Verifier

In this module third party auditor has to respond the auditing report based on the data owners requests.

INPUT DESIGN & OUTPUT DESIGN

GIVEN INPUT AND EXPECTED OUTPUT

Authentication:

Input: Register the user Details and give the username and Password to login

Output: They will be granted to access the data's

Group Manager:

Input: Authorized person enter the details and get the allocation from Cloud.

Output: Give the permission to store the data.

Cloud Process:

Input: Allow the registration user and block revoke users.

Output: to get the details from the cloud and access.

Maintain Revocation List:

Input: Get the resignation user details from company maintain revoke list.

Output: Cannot allow accessing the cloud storage data's.

Maintain Access Control List:

Input: Collect the register user details from the company and maintain the Access control list.

Output: Get the access control from the cloud

New User:

Input: To provide the access control to the new users.

Output: Allow to access and update the cloud.

Third Party Auditor

Input: Auditing request

Output: Auditing Response

TECHNIQUE USED

Key-update cloud service provider (KU-CSP)

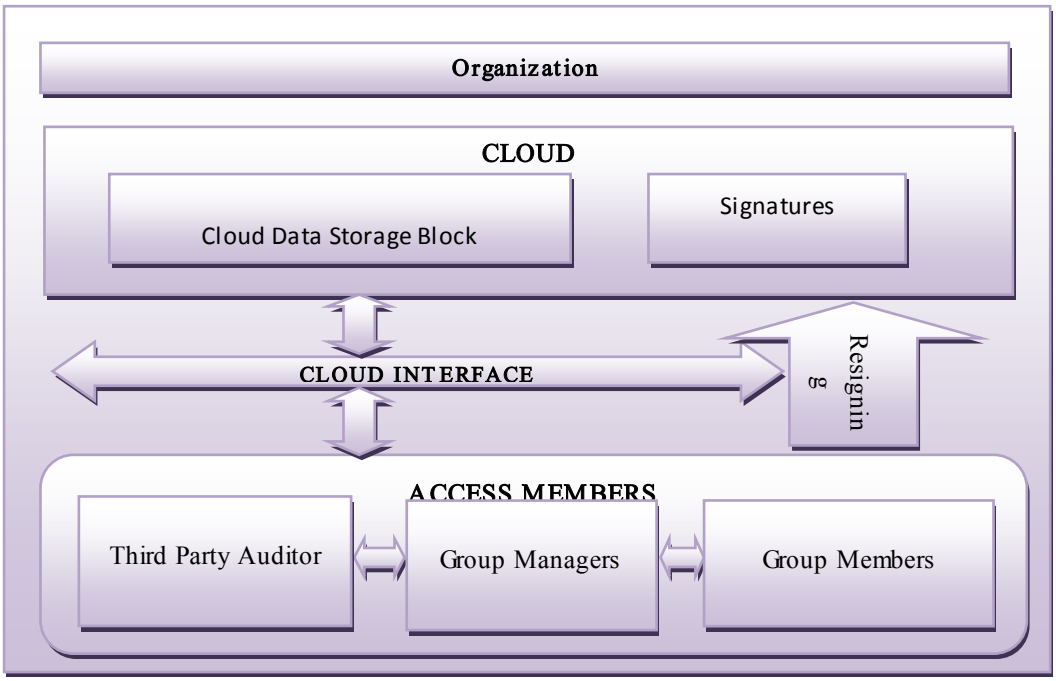
A revocable IBE scheme with a key-update cloud service provider (KU-CSP). They shift the key-update procedures to a KU-CSP to alleviate the load of PKG. The KUCSP generates the current time update key of a user by using the associated time key and sends it to the user via a public channel. To revoke a user, to stop issuing the new time update key of the user.

SYSTEM DESIGN

Design Engineering deals with the various UML [Unified Modeling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the

means to accurately translate customer requirements into finished product.

3. SYSTEM ARCHITECTURE



Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script.

".NET" is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

SQL SERVER 2012:

SQL Server 2005 will be soon reaching its three-year mark, which in terms of software life-cycle translates into fairly advanced maturity. While this is still far from retirement age, the name of its successor, SQL Server 2008, suggests that it might be time for you to start looking into what the new generation has to offer. The release of SQL Server 2008, originally introduced as Yukon, has already been postponed, but its current Beta 2 implementation (with several incremental Community Technical Previews expected before Beta 3 becomes available early next year) brings promise of a timely RTM stage (planned for summer next year). In this series of articles, we will look into functional highlights of the new

incarnation of the Microsoft database management system, focusing on those that are likely to remain unchanged in the final product.

5. APPLICATION

It can be applied to the following areas

- Economic Related Application.
- Outsourcing Based Applications.
- Cloud Based Application.

6. CONCLUSION

In this paper, we proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation

7. REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Crypto'84, LNCS, vol. 196, pp. 47-53, 1984.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the

[3]R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 3280, 2002.

[4] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," Proc. Crypto'98, LNCS, vol. 1462, pp. 137-152, 1998.

[5] S. Micali, "Novomodo: Scalable certificate validation and simplified PKI management," Proc. 1st Annual PKI Research Workshop, pp. 15-25, 2002.

[6] F. F. Elwailly, C. Gentry, and Z. Ramzan, "QuasiModo: Efficient certificate validation and revocation," Proc. PKC'04, LNCS, vol. 2947, pp. 375-388, 2004.

[7] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," Proc. Financial Cryptography, LNCS, vol. 4886, pp. 247-259, 2007.

[8] D. Boneh, X. Ding, G. Tsudik, and C.-M. Wong, "A Method for fast revocation of public key certificates and security capabilities," Proc. 10th USENIX Security Symp., pp. 297-310. 2001.