iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33744

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Attribute Based Access Control for Mobile Clouds without Proxy Outsourcing

Ms. M. Bavithra[1], Mr. V. Visu[2]
[1]*Assistant Professor, Department of MCA, Dhnalakshmi Srinivasan EngineeringCollege, Perambalur, Tamil Nadu.*
[2]*Master of computer Applications, Dhanalakshmi Srinivasan EngineeringCollege, Perambalur, Tamil Nadu.*

Abstract: ***Fine grained access control is a requirement for data stored in untrusted servers like clouds. Owing to the large volume of data, decentralized key management schemes are preferred over centralized ones. Often encryption and decryption are quite expensive. In existing system a decentralized attribute based encryption (ABE) scheme with fast encryption, outsourced decryption and user revocation. This out sourcing paves a way for security leak. In proposed system the attribute based encryption is enhanced and decryption is done without proxy outsourcing. The metadata and dynamic attributes are used for decryption which provides robust security.***
Keywords: Attribute-based encryption, Key management, Encryption and decryption.

I. INTRODUCTION

Consider the common scenario where data owners want to upload their data for long-term storage to untrusted servers such as the cloud. The data may initially reside in resource constrained devices such as mobile phones, wireless sensors or smartcards. The aim is to store the data over a long time and allow multiple users to access the data. Cloud Service Providers (CSPs) today provide such seemingly unlimited storage facilities and are thurapidly gaining popularity among individual data owners as well as enterprises with limited budgets.

In spite of the benefits provided by CSPs, they are assumed to be malicious and data owners generally do not trust them with their sensitive data. So, any data stored in the cloud must be encrypted. Moreover, data owners may wish to impose access control measures on data so that only users who have certain credentials can access it.

For example, a hospital may wish to upload to the cloud the results of a clinical trial recording the response of cancer patients to a new drug. This data is sensitive and the hospital may want only the doctor attending a patient or a researcher involved in the drug discovery to have access to the data.

Encryption schemes such as attribute-based encryption (ABE) provide great flexibility in terms of access control on encrypted data and are ideal for this scenario. In practice, decentralized or multi-authority ABE schemes are very useful as they do not need any central authority for generation and distribution of decryption keys related to different attributes. For example, the doctor who wants to access a patient's health record for diagnosis may be provided the relevant key by the hospital but a medical researcher may be given access to the same data by a medical research organization. User attributes are subject to periodic changes due change in the work environment, location etc.

Thus, a user who was previously granted access to data may no longer qualify for the access. Unless previously allotted keys are updated and the user is revoked, the user may continue to access the data in spite of a change in his attributes. So, user revocation is a necessary and useful property for ABE schemes

II. PROPOSED ALGORITHM

In proposed system the attribute based encryption is enhanced.The decryption is done without proxy out sourcing. The metadata and dynamic attributes are used for decryption which provides robust security.

A. Focal Point

The system supports user revocation without incurring much additional cost in the online phase. Overall, unlike other existing works, our scheme hits a good balance between encryption and decryption performance, while supporting additional useful properties such as decentralization and user revocation.

©IJRASET: All Rights are Reserved

III. ENVIRONMENT DETAILS

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use.

1) Software Specification

a) Front end =java 8 and above
b) Back end =MySql 5 and above
c) Tool =netbeans 8.0 and above

2) Hardware Specification

a) Processor =Intel i3 and above
b) Ram =4 GB and above
c) Hard disk =250 GB and above

A. System Architecture

1) Cloud Server Creation

a) A cloud server is created
b) Users will be registered in cloud server.
c) User data are stored In the server. Then data and resources are uploaded for user need are handled. Then the data synchronized to the open access devicewhereeasy access allocated to the users in a open accessibility mode.

2) Multi-Authority Ciphertext-Policy Attribute Based Encryption

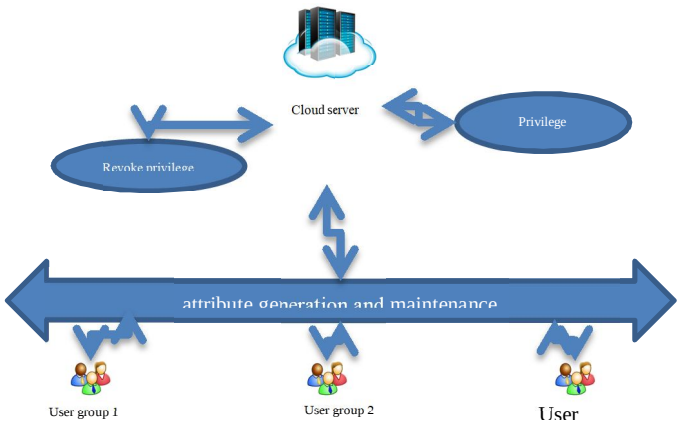
a) A multi authorized cloud encryption is allocated for the user data.
b) Cost maintenance for different cloud will be done.

3) Security Provision Decryption

a) High level security is provided for cloud data
b) And the ciphered data is deciphered. A secured decryption is done.
c) In order to prove the security of the of Online/Offline Multi-Authority CPABE with Outsourced Decryption (OO-MA-DO-CPABE), we consider the intermediate scheme Online/Offline Multi-Authority CPABE (OO-MACPABE) without decryption outsourcing.

4) Retiving Original Data

a) A secured data is obtained by decryption method.
b) The original user data is retrieved.
c) ABE scheme suitable for mobile clouds. It combines the useful properties of decentralization, fast encryption, outsourced decryption and user revocation.
d) All heavy computations related to encryption are performed during the offline phase making the whole encryption phase faster and more efficient than existing decentralized ABE schemes.



©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

B. Software Overview

Java is a platform Independent. Java is a high level programming language Introduced by Sun Microsystems in June 1995 Java is becoming a standard for Internet Applications. It provides for interactive processing and for the use of graphics and animation on the Internet.

Since the Internet consists of different types of computers and operating systems, a common language was needed to enable computers to run programs that run on multiple platforms. Java is an object oriented language built upon C and C++.It derives its syntax from C and its object-oriented features are influenced by C++. Java can be used to create applications and applets. An application is a program that runs on the user's computer, under its operating system.

An applet is a small window based program that runs on HTML page using Java enabled browser like Internet Explorer, Netscape Navigator, Hot Java or an applet view

1) Features of JAVA

Simple

a) Java Language constructs are easy to learn and use. It takes care of memory management. Though

b) Java was developed from C++, the complexities associated with C++ have been eliminated in Java.

2) Object-Oriented: Java is designed around the object-oriented model. In Java the focus is on the 'data' and the 'methods' that operate on the data in an application and not just on the procedures. The data and methods together describe the state and the behaviour of an object in Java

3) Robust: Java is a robust language since it has strict compile time and run time checking of code. This minimizes programming errors. Error handling and recovery is taken care of in Java by the 'exception- handling' feature.

4) Secure: Java is language that focuses on the network. Java security features ensure that its programs that run are safe. Programmers cannot manipulate memory in Java. This is a good defense mechanism against malicious code that may flow in from the network. Java programs running on the Web cannot open, read, write or delete files on the user's system or run other programs on it.

5) Distributed: Java can be used to develop applications that are portable across multiple platforms, operating systems and graphical user interfaces. Java is designed to support network applications. Thus Java is widely used tool in an environment like the Internet where there are different platforms.

6) Multithreaded: Java programs can do many tasks simultaneously by a process called 'multithreading'. Java provides the master solution for synchronizing multiple processes. Therefore, interactive applications on the Net can run smoothly. This is made possible by the built-in support for threads.

- Running Java File with single command
- New utility methods in String class
- Local-Variable Syntax for Lambda Parameters
- Nested Based Access Control
- HTTP Client
- Reading/Writing Strings to and from the Files
- Flight Recorder

C. Technology infrastructure

CORE JAVA: Java can be used to create two types of programs: application and applet. An application is a program that runs on your computer, under the operating system of that computer. That is, an application created by java is more or less like one created using C or C++.

When used to create application, java is not much different from any other computer language. Rather, it is java's ability to create applets that makes it important. An applet is an application designed to be transmitted over the internet and executed by a java-compatible Web Browser.

An applet is actually a tiny java program, dynamically downloaded across the network, just like an image, sound file, or video clip. The important difference is that an applet is an intelligent program, not just an animation or media file.

In other words, an applet is a program that can react to user input and dynamically change-not just run the same animation or sound over and over.

©IJRASET: All Rights are Reserved

D. Developing Metholodies

The test process is initiated by developing a comprehensive plan to test the general functionality and special features on a variety of platform combinations. Strict quality control procedures are used. The process verifies that the application meets the requirements specified in the system requirements document and is bug free. The following are the considerations used to develop the framework from developing the testing methodologies

IV. CONCLUSION

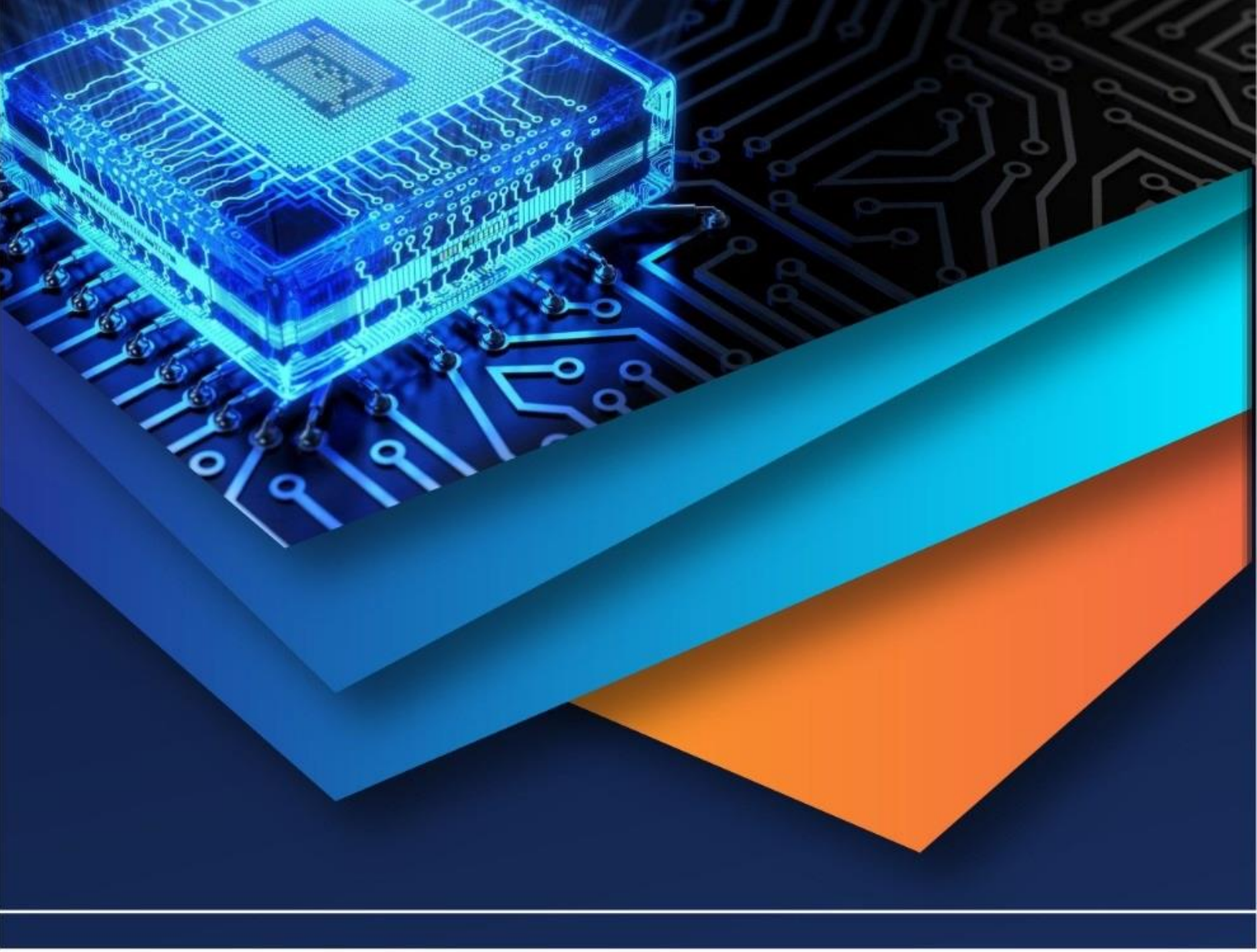
The proposed system propose an ABE scheme suitable for mobile clouds. It combines the useful properties of decentralization, fast encryption, outsourced decryption and user revocation. All heavy computations related to encryption are performed during the offline phase making the whole encryption phase faster and more efficient than existing decentralized ABE schemes. An untrusted proxy server partially decrypts the ciphertext without gaining any information about the plaintext. Data users can then fully decrypt the partially decrypted ciphertext without performing any costly pairing operations. the scheme supports user revocation without incurring much additional cost in the online phase. Overall, unlike other existing works, our scheme hits a good balance between encryption and decryption performance, while supporting additional useful properties such as decentralization and user revocation.

REFERENCES

[1] N. Attrapadung and H. Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278– 300. Springer, 2009.
[2] N. Attrapadung and H. Imai. Conjunctive broadcast and attribute-based encryption. In Pairing-Based Cryptography-Pairing 2009: Third International Conference Palo Alto, CA, USA, August 12-14, 2009 Proceedings, volume 5671, page 248. Springer Science & Business Media, 2009.
[3] N. Balani and S. Ruj. Temporal access control with user revocation for cloud data. In 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing,China, September 24-26, 2014, pages 336–343, 2014.
[4] A. Beimel. Secure schemes for secret sharing and key distribution. Ph.D. Thesis, Israel Institute of Technolgy, Technion, Haifa, Israel, 1996.
[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pages 321–334. IEEE Computer Society, 2007
[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In Proceedings of the 15th ACM conference on Computer and communications security, pages 417–426. ACM, 2008.
[7] R. Canetti, H. Krawczyk, and J. B. Nielsen. Relaxing chosen-ciphertext security. In D. Boneh, editor, Advances in Cryptology - CRYPTO 2003, 23rdAnnual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 565–582. Springer, 2003.
[8] M. Chase. Multi-authority attribute based encryption. In Proceedings ofTheory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007 [8], pages 515– 534.
[9] M. Chase and S. S. M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009 [9], pages 121–130.
[10] CryptoExperts. ABC4Trust. https://www.cryptoexperts.com/research/ projects/abc4trust/. Accessed: 2015-03-28.

.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)