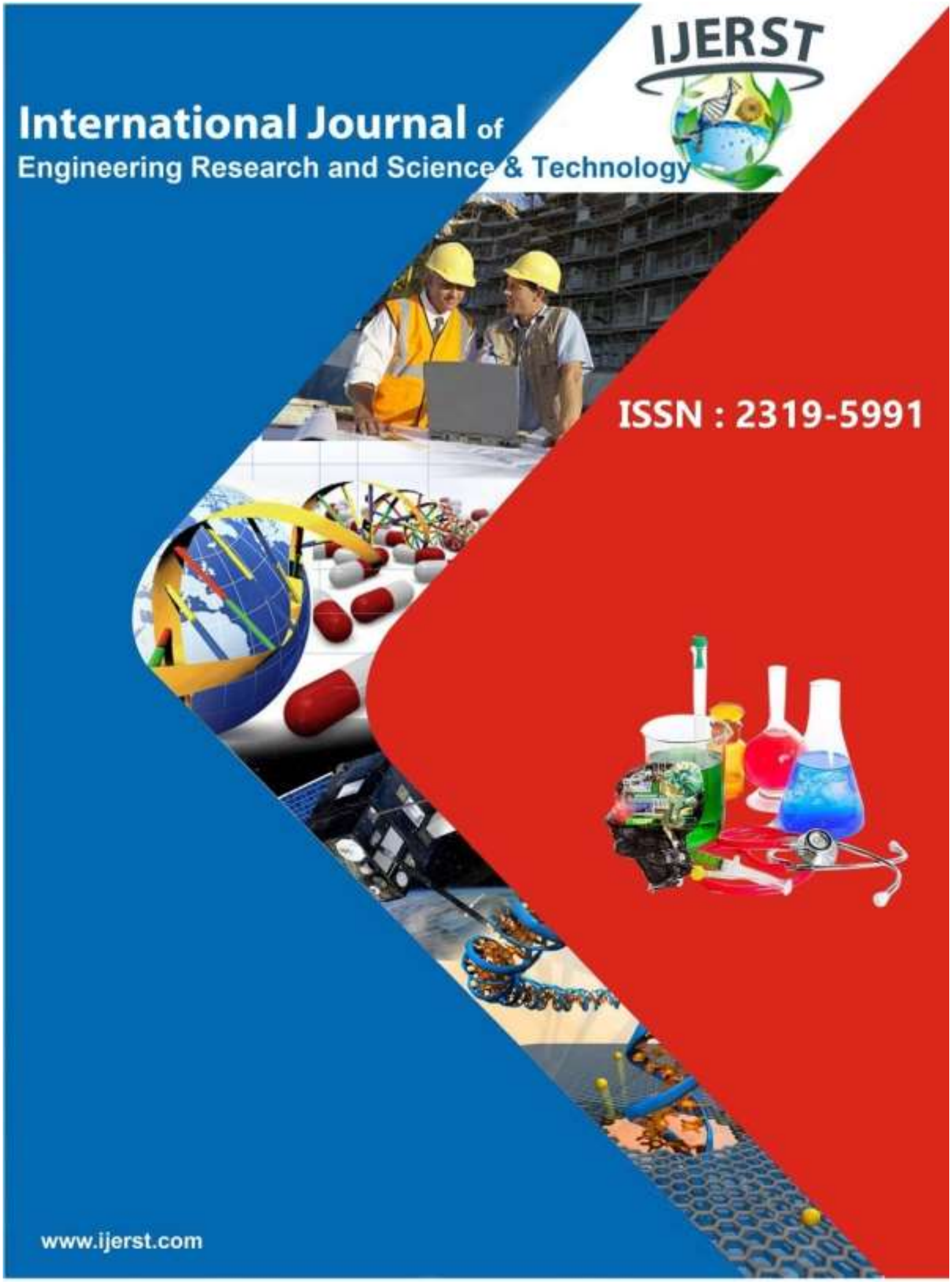


IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

Vol. 11, Issuse.2,April 2023

SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE

Mrs.D.Aiswarya [1],Vereedhi Rama Naga Anjani [2],Tankasala Aishwarya [3],Kudipudi Lakshmi Sai Shanmukh [4],Sunkara Bhuvaneswari [5],Manam Suryanarayana [6]

ABSTRACT

Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credentials (i.e. decryption rights), due to the intrinsic "all-or-nothing" decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi-trusted authority side, and the other is on the side of cloud users. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as CryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

Keywords: Secure Cloud Storage, Cipher, Access Credentials Misuse, Traceability and Revocation, Auditing.

1.INTRODUCTION

The prevalence of cloud computing may indirectly incur vulnerability to the confidentiality of outsourced data and the privacy of cloud users. A particular challenge here is on how to guarantee that only authorized users can gain access to the data, which has been outsourced to the cloud, at anywhere and anytime. One naive solution is to employ encryption techniques on the data prior to uploading to the cloud. However, the solution limits further data sharing and processing.

This is so because a data owner needs to download the encrypted data from the cloud and further re-encrypt them for sharing (suppose the data owner has no local copies of the data). A fine-grained access control over encrypted data is desirable in the context of cloud computing. Ciphertext-Policy Attribute-Based Encryption (CPABE) may be an effective solution to guarantee the confidentiality of data and provide fine-grained access control here. In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user.

Authorized cloud users are then granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data.

As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in the cloud, but also enables fine-grained access control over the data. Generally speaking, the existing CP-ABE based cloud storage systems fail to consider the case where access credential is misused. For instance, a university deploys a CP ABE based cloud storage system to outsource encrypted student data to cloud under some access policies that are compliant with the relevant data sharing and privacy legislation (e.g., the federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act of 1992 (HIPAA)). The official in charge at the organization (e.g. university's security manager) initializes the system parameters and issues access credentials for all users (e.g., students, faculty members, and visiting scholars). Each employee is assigned with several attributes (e.g., "administrator", "senior manager", "financial officer", "tenured faculty", "tenure-track faculty", "non tenure-track faculty", "instructors", "adjunct", "visitor", and/or "students"). Only the employees with attributes satisfying the decryption policy of the outsourced data are able to gain access to the student data stored in cloud (e.g. student admission materials).

2. LITERATURE SURVEY

Cloud computing exhibits remarkable potential to provide cost effective, easy to manage, elastic, and powerful resources on the fly, over the Internet. Cloud computing, upsurges the capabilities of the hardware resources by optimal and shared utilization. The above mentioned features encourage the organizations and individual users to shift their applications and services to the cloud. Even the critical infrastructure, for example, power generation and distribution plants are being migrated to the cloud computing paradigm. However, the services provided by third-party cloud service providers entail additional security threats. The migration of user's assets (data, applications etc.) outside the administrative control in a shared environment where numerous users are collocated escalates the security concerns. This survey details the security issues that arise due to the very nature of cloud computing. Moreover, the survey presents the recent solutions presented in the literature to counter the security issues. Furthermore, a brief view of security vulnerabilities in the mobile cloud computing are also highlighted. In the end, the discussion on the open issues and future research directions is also presented.

3. EXISTING SYSTEM

Cloud storage explores new applications of data storage, so that data owners do take full responsibility of data management "in local" no more. However, due to the separation of data ownership and data access in cloud settings, the management of data, software, physical machines and platforms need to be delegated to cloud service providers, so that data owner only maintains little control on virtual machines.

To protect the confidentiality of cloud data, many cloud based fine-grained access control systems have been introduced in the literature. Searchable encryption enables secure search over ciphertexts by using the predefined keywords. The data audit and deduplication enables users to check the integrity of the outsourced data and to remove storage redundancy

DISADVANTAGES OF EXISTING SYSTEM

The main disadvantage of the existing system is LESSER SECURITY.This proposed system is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, Crypt Cloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority.

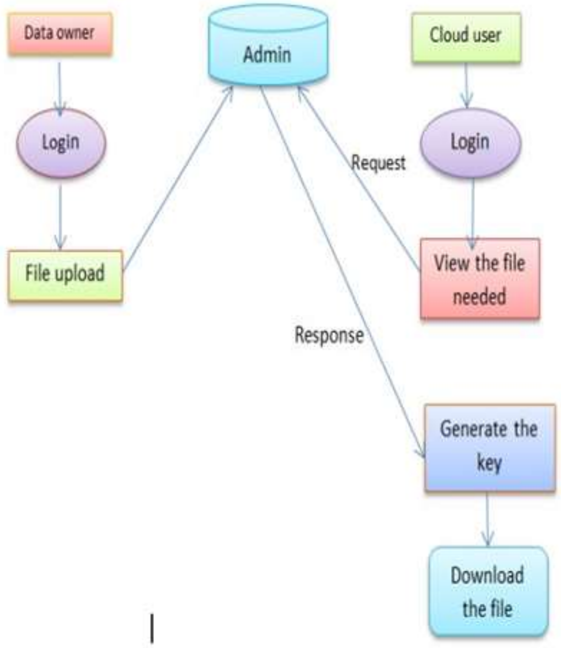
PROPOSED SYSTEM

Based on ATER-CP-ABE and ATIR-CP-ABE, we propose the CryptCloud+. The system works as follows. AT first generates the system parameters to set up the system and shares the entire system parameters (including public and private parameters) with AU. It then publishes the public parameters. Also, AT generates access credentials (i.e. decryption keys) for DUs according to their identities and attributes. DOs encrypt their data under access policies and then outsource the encrypted data to the PC.

Any authorized DU is able to decrypt the outsourced ciphertexts to access the underlying data. A DU is authorized if the set of attributes he/she possesses satisfies the access policy defined over the outsourced data. At some point, a legitimate access credential may be sold online, such as in an underground forum. As long as the credential is located or when a DO sends a trace request AU calls the trace procedure to identify the traitor. If there exists a DU being identified as the traitor but claims to be innocent, then AU may call the audit procedure to make a judgment.

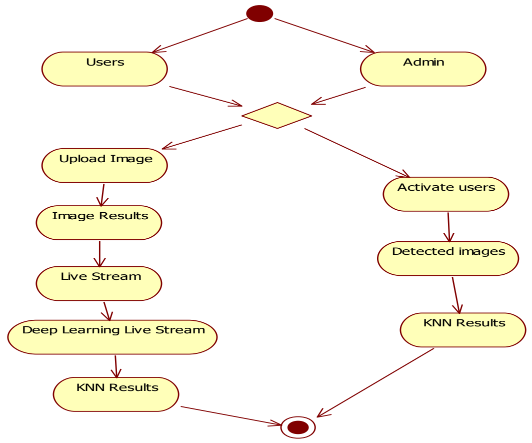
4.SYSTEM ARCHITECTURE .

Below diagram depicts the whole system architecture of the project



Activity Diagram

A graphical representations of work process of stepwise exercises and activities with support for decision, emphasis and simultaneousness, used to depict the business and operational well-ordered stream of parts in a framework furthermore demonstrates the general stream of control.



5. SYSTEM IMPLEMENTATION

There are 5 modules: 1.Data User 2.Data Owner 3.Cloud 4.Authority 5.Auditor

Data Owner:-

Ø Register Ø Login

Ø Upload Files Ø View files

Ø My Profile Ø Logout

Data User:-

Ø Register Ø Login

Ø Search Files

Ø My Downloads Ø My Profile

Ø Logout

Cloud:-

Ø Login

Ø Data Owner

Ø Data User Ø Data Access Ø Logout

Authority:-

Ø Login

Ø Data Credential

Auditor:-

Ø Login

Ø Attacked Files Ø Trace Files

6.TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6.1 TYPES OF TESTING

■ Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

■ Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

■ Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

7.RESULTS

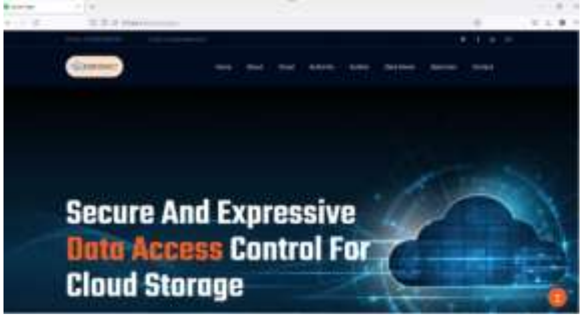


Fig :home screen

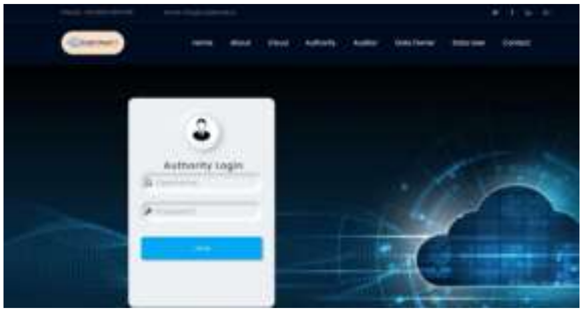


Fig :Authority Login

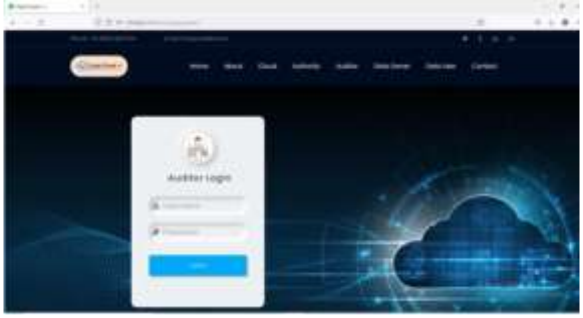


Fig : Auditor Login

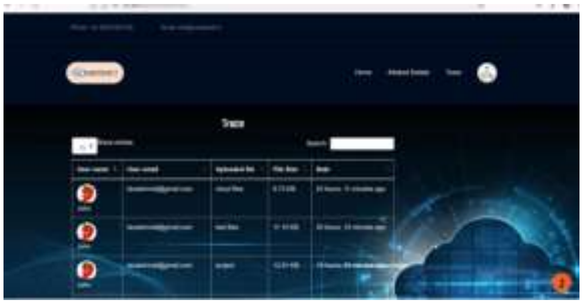


Fig : This figure shows traced files

8. CONCLUSION & FUTURE WORK

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable CryptCloud which supports white-box traceability and auditing (referred to as CryptCloud+). This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, CryptCloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority. We note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in CryptCloud. One of our future works is to consider the black-box traceability and auditing. Furthermore, AU is assumed to be fully trusted in CryptCloud+. However, in practice, it may not be the case. Is there any way to reduce trust from AU? Intuitively, one method is to employ multiple AUs.

This is similar to the technique used in threshold schemes. But it will require additional communication and deployment cost and meanwhile, the problem of collusion among AUs remains. Another potential approach is to employ secure multi-party computation in the presence of malicious adversaries. However, the efficiency is also a bottleneck. Designing efficient multi-party computation and decentralizing trust among AUs (while maintaining the same level of security and efficiency) is also a part of our future work. We use Paillier-like encryption to serve as an extractable commitment to achieve white-box traceability. From an abstract view point, any extractable commitment may be employed to achieve white-box traceability in theory.

To improve the efficiency of tracing, we may make use of a more light-weight (pairing-suitable) extractable commitment. Also, the trace algorithm in

CryptCloud+ needs to take the master secret key as input to achieve white-box traceability of malicious cloud users. Intuitively, the proposed CryptCloud+ is private traceable5 . Private traceability only allows the tracing algorithm to be run by the system administrator itself, while partial/full public traceability enables the administrator, authorized users and even anyone without the secret information of the system to fulfill the trace. Our future work will include extending CryptCloud+ to provide "partial" and fully public traceability without compromising on performance.

REFERENCES

[1]Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert
Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

[2]Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3]Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4]Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[5]Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[6]Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.

[7]Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8]Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.

[9]Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.