IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ATTRIBUTE-BASED ENCRYPTION FOR FINE-GRAINED DATA ACCESS IN CLOUD COMPUTING

Jaya Priya P[1], Pavithra A [2]

[1]Jaya Priya P M.Sc, Department of Computer Science and Engineering, Dr. MGR Educational and Research Institute, Chennai, India

[2]Pavithra A Faculty, Centre of Excellence in Digital Forensics, Dr. MGR Educational and Research Institute, Chennai, India

ABSTRACT:

An upcoming cloud service called "secure cloud storage" is meant to safeguard the privacy of data that is outsourced while also giving cloud users who have data that is not under their physical control flexible access. Policy Attribute-Based Encryption (CP-ABE) with cipher text is considered one of the most promising methods that may be used to ensure service guarantee security. However, because of CP-ABE's inherent "all-or-nothing" decryption characteristic, using it may inevitably result in a security compromise known as the misuse of access credentials (i.e., decryption privileges). This project looks into two primary scenarios of access credential misuse in this paper: one involves a semi-trusted authority and the other involves a cloud user. Our proposal, called Crypt Cloud, is the first responsible authority and revocable cloud storage solution based on CP-ABE with white-box traceability and auditing to reduce misuse. Additionally, it provides the security analysis and use experiments to show off our system's usefulness.

Keywords:

J2EE (JSP, Servlets), JavaScript, HTML, CSS, AJAX

INTRODUCTION

Ensuring the integrity of an organization's data stored in a public cloud is the primary goal of this project. Owners of data will keep it in public clouds, protected by encryption and certain features that allow control over who can access it. They will give their data an attribute set when they upload it to the public cloud. Any authorized cloud user who want to download their data must enter that specific attribute set in order to access the data owner's data and take other actions. In order to access the data owner's information, a cloud user wishes to register their information with the cloud organization. Users wish to provide their designation and personal information as characteristic**.** based on the user's information The Semi-Trusted Authority creates decryption keys in order to obtain ownership over the data. Numerous procedures can be carried out by a user on cloud data. The user must input certain read-related qualities if he wishes to read the cloud data, and write-related attributes if he wants to write the data. Users in an organization would be validated using their own set of attributes prior to each and every operation. The administrators in a cloud organization would share these attributes with the permitted users. These characteristics will be kept in cloud-based policy files. In the event that a user divulges their special decryption key to a malevolent party, data owners wish to investigate by submitting an audit request to the auditor, who will examine the data owner's request and determine the offending party.

REVIEW OF LITERATURE

Java has been around since 1991, developed by a small platoon of Sun Microsystems inventors in a design firstly called the Green design. The intent of the design was to develop a platform-independent software technology that would be used in consumer electronics assiduity. The language that the platoon created was first called Oak.

The first performance of Oak was in a PDA- type device called Star Seven(* 7) that comported of the Oak language, an operating system called GreenOS, a stoner interface, and attack. The name * 7 was deduced from the telephone sequence that was used in the platoon's office and that was telephoned in order to answer any ringing telephone from any other phone in the office.

Around the time the First Person design was floundering in consumer electronics, a new mode was gaining instigation in America; the mode was called" Web surfing." The World Wide Web, a name applied to the Internet's millions of linked HTML documents was suddenly getting popular for use by the millions. The reason for this was the foreword of a graphical Web cybersurfer called Mosaic, developed by NCSA. The cybersurfer simplified Web browsing by combining textbooks and plates into a single interface to count the need for addicts to learn numerous confusing UNIX and DOS commands. Navigating around the Web was much easier using Mosaic.

It has only been since 1994 that Oak technology has been applied to the Web. In 1994, two Sun inventors created the first interpretation of Hot Java, also called Web Runner, a graphical cybersurfer for the Web that exists moment. The cybersurfer was enciphered entirely in the Oak language, called Java. Soon subsequently, the Java compiler was rewritten in the Java language from its original C law, proving that Java could be used effectively as an operation language. Sun introduced Java in May 1995 at the Sun World 95 convention.

Web surfing has become a considerably popular practice among millions of computer addicts. Until Java, still, the content of information on the Internet has been a mellow series of HTML documents. Web addicts are empty for operations that are interactive, that addicts can execute no matter what attack or software platform they're using, and that trip across miscellaneous networks and don't spread contagions to their computers. Java can produce a similar application

RESEARCH METHODOLOGY

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 how to guarantee that only authorized users can gain access to the data, which has been outsourced to cloud, anywhere and at any time. One naive solution is to employ encryption techniques on the data before uploading it to the cloud. Nevertheless, the solution restricts additional data processing and sharing. This is the case because, assuming the data owner has no local copies, they must download the encrypted data from the cloud and re-encrypt it before sharing it. In cloud computing, a more precise access control over encrypted data is preferred.

Here, cipher text Policy Attribute-Based Encryption (CPABE) might be useful to ensure data privacy and offer fine-grained access control. Organizations (like the University of Texas at San Antonio) and individuals (like students, faculty, and visiting scholars) can first specify access policy over attributes of a potential cloud user in a CP-ABE-based cloud storage system, for example. After that, authorized cloud users are given access credentials (i.e., decryption keys) that match their attribute sets (e.g., visitor role, faculty member role, or student role), which they can use to access the data that has been outsourced 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 cloud but also enables fine-grained access control over the data

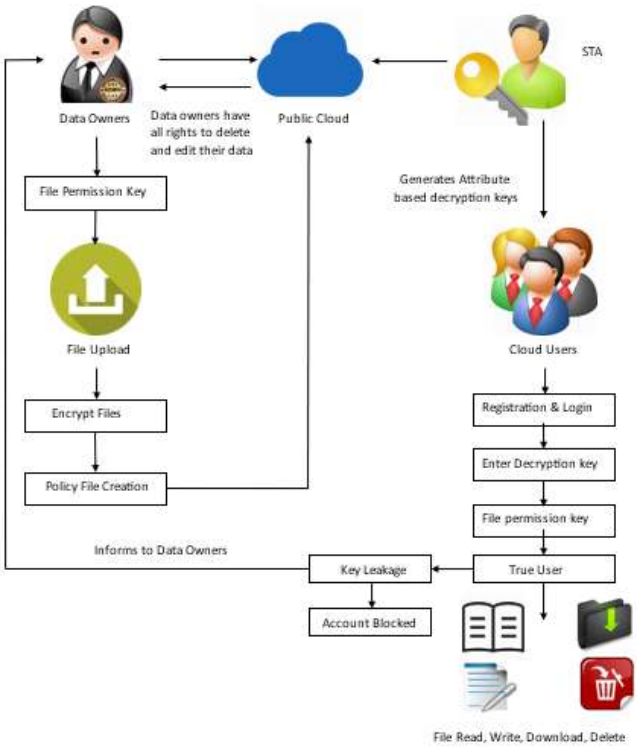

Fig 1 Safety Diagram

3.1 Organization Profile Creation & Key Generation

At the web end, there is a basic registration process for users. For this process, the users supply their own personal information. The data is then kept on the server in its database. Users now receive decryption keys from the Accountable STA (semi-trusted Authority) based on their Attributes Set (name, email address, phone number, etc.). After receiving the decryption keys from the Accountable STA, the user has the provenance to access the Organization's data.

3.2 Data Owners File Upload

In this module data owners create their accounts under the public cloud and upload their data into public cloud. While uploading the files into the public cloud data owners will encrypt their data using RSA Encryption algorithm and generates public key and secret key. And also generates one unique file access permission key for the users under the organization to access their data

3.3 File Permission & Policy File Creation

Various data owners will create unique file permission keys for their files, which they then provide to users inside the company so they can access their files. Additionally, it creates policy files for their data to control who has access to it. The policy file will separate the keys for downloading, writing, reading, and deleting files.

3.4 Tracing who is guilty:

The outsourced data can be accessed by authorized DUs in a number of ways, including read, write, download, delete, and decrypt. Employees within the company are given file permission keys here according to their position and experience. All-access permissions to the files (read, write, delete, and download) are granted to senior employees. The only permission granted to freshers is to read the files. Certain employees are authorized to read and write. Furthermore, some workers are fully authorized to do everything but erase the data. Senior Employees will be asked to download or erase the Data Owners' Data if they leak information or give their confidential permission keys to their junior colleagues. As the user enters the key, the system will automatically generate an attribute set specific to their role and verify that they possess all necessary

rights to access the data. They will be held accountable if the attributes set does not match the Data Owners policy files. The project can find out who gave the junior employees access to the key if it asks them.

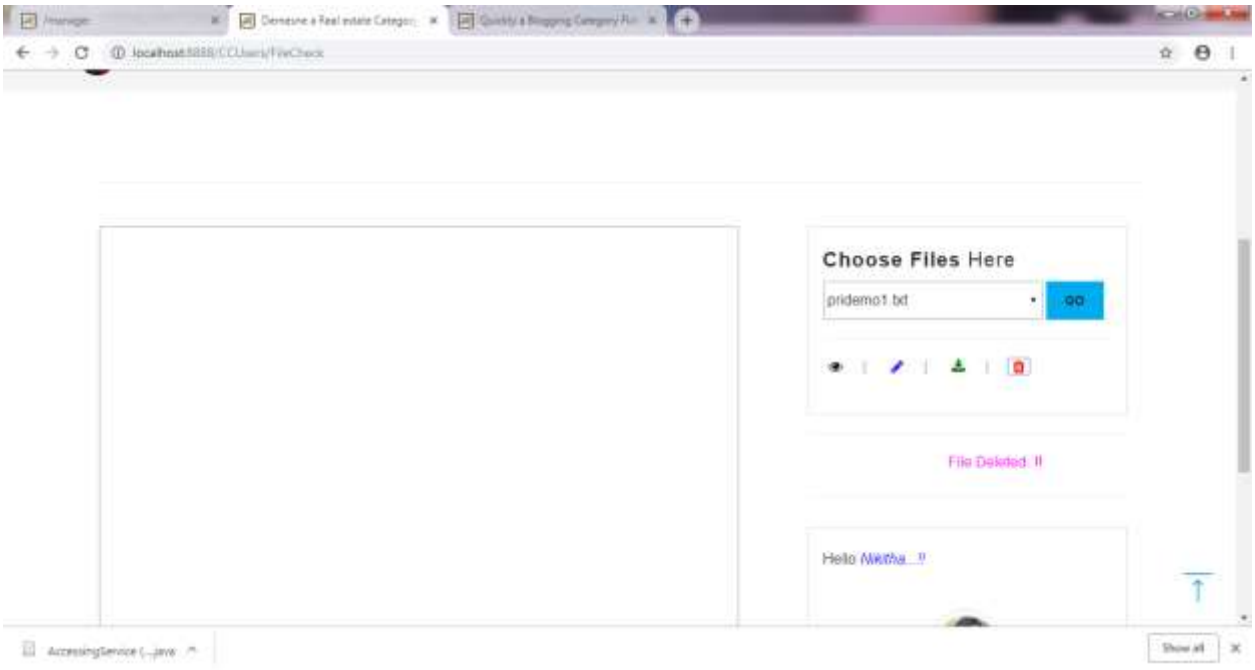

Fig 2: Cloud Security File Model

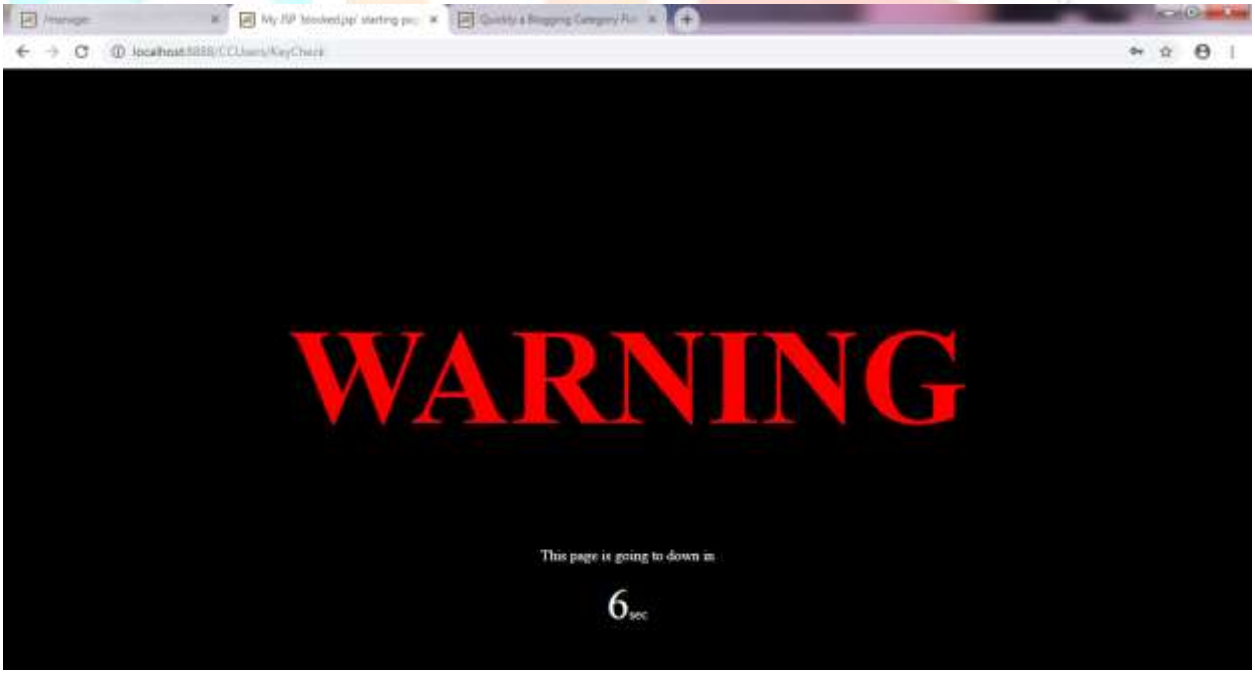

Fig 3: Keys

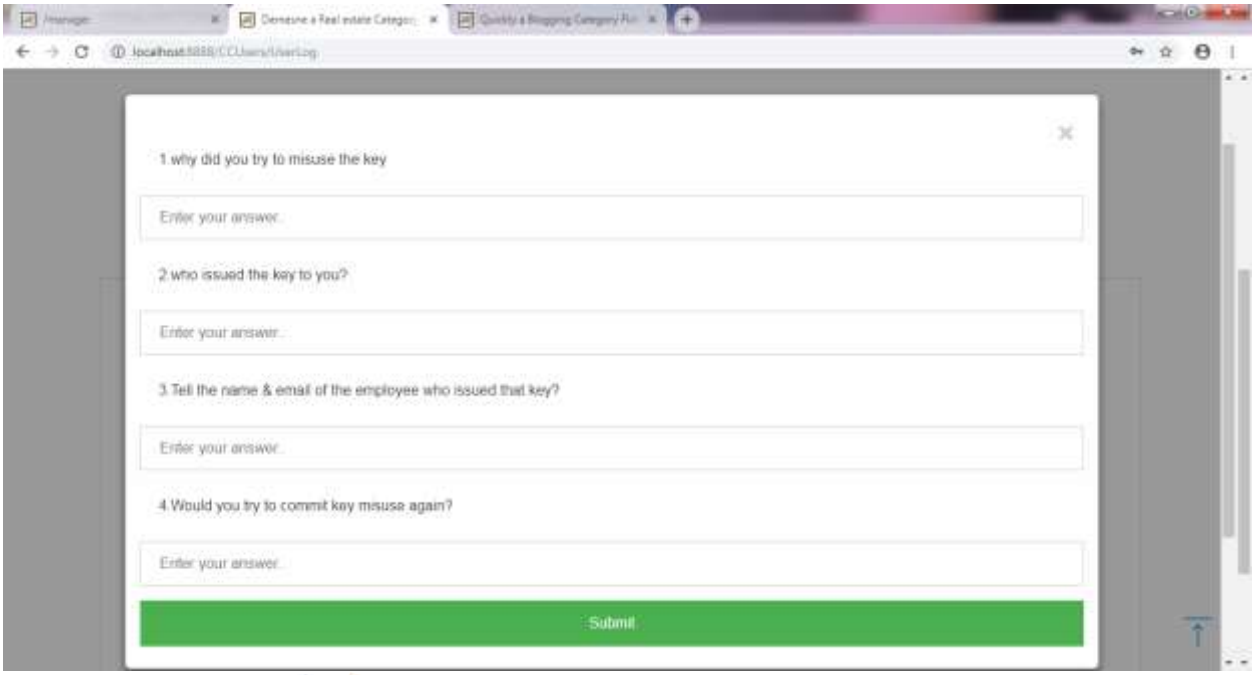

Fig 4: Authority

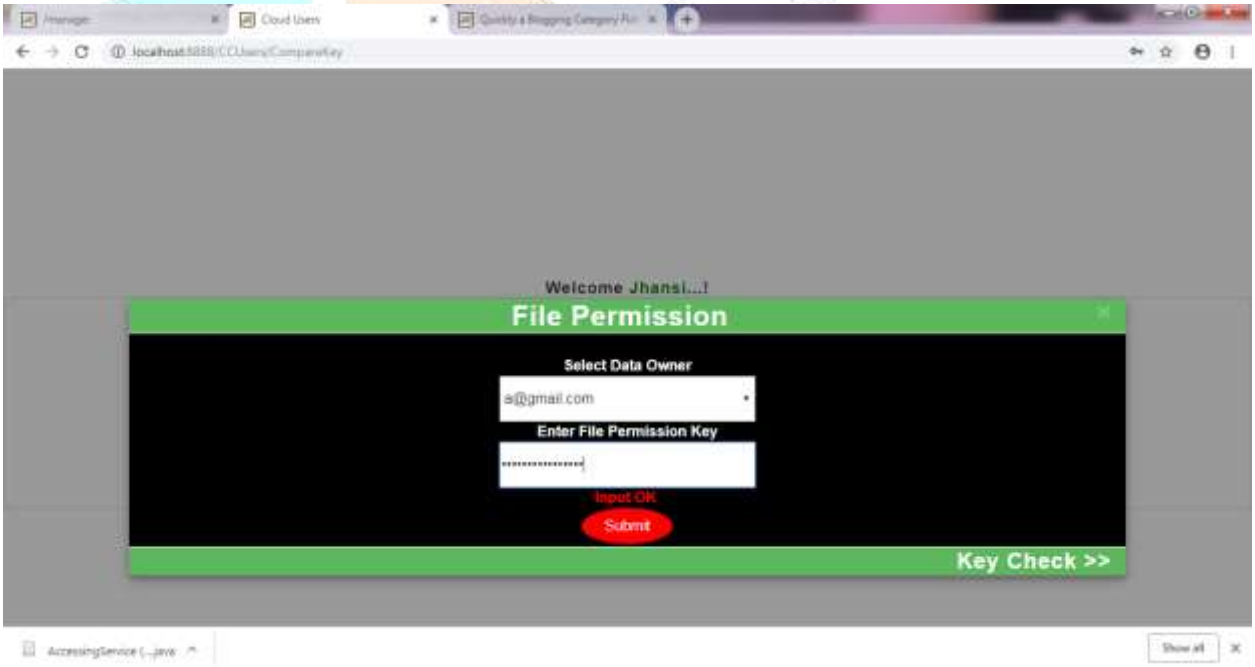

Fig 5: Owner Login

Conclusion

In this work, it has addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing (referred to as CryptCloud+). This is the first cloud storage system built on CP-ABE that can support auditing, effective revocation, accountable authority, and white-box traceability all at the same time. 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. We note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in CryptCloud. Our next project will look into auditing and black-box traceability.

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, R ean 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.

[11]. Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.

[12]. Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.

[13]. Vipul Goyal. Reducing trust in the PKG in identity based cryptosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447. Springer, 2007.

[14]. Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008