Authenticating a Java Archive files using Identity Based Encryption in the Cloud

Ms R.PUNITHA
II year ME
Department of Computer Science Engg
Erode Sengunthar Engg College-erode
punitha.me2011@gmail.com

Mr.D.VIJAYBABU
Assistant Professor
Department of Computer Science Engg
Erode Sengunthar Engg College-erode
mani.babu2008@gmail.com

ABSTRACT

Cloud computing is one of the most modern research areas due to its ability to decrease costs coupled with computing while growing scalability and flexibility for computing services. Cloud computing is one of the greatest increasing technology of the IT trade for business. Since cloud computing share distributed resources through the network in the open environment, hence it makes security problems very important for us to develop the cloud computing applications. So that they wanted to account their data,which are stored in cloud. It can make available accountability for cloud data by using a framework called Cloud Information Accountability (CIA). Here it uses Java Archives (JAR) files for automatically log the usage of user's data. To support user's control, it can provide distributed auditing mechanism. So data also encrypted in this scheme Hierarchical identity based encryption (HIBE). In this method various significant security services including compression, encryption and authentication also.

Index terms

Cloud computing; Cloud security; Accountability; Data sharing; JAR file; HIBE;

1. INTRODUCTION

A cloud is normally contains a virtualized major part of the computing resources, which could be reallocated to the different purposes within short time periods. The whole process of requesting and receiving resources is typically automated and is completed in minutes. The cloud computing is the set of software, hardware, networks, storage, services and interfaces that combines to deliver aspects of the cloud computing as a service. Share resources, software and information are provided to computers and other devices on demand. It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology.

Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic. The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a standard browser.

IJERT

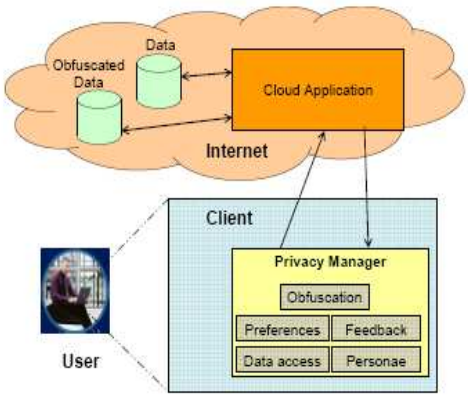

Fig: 1 cloud computing usage

From the viewpoint of data security, which has always been an important part of quality of service, Cloud Computing certainly positions a new challenging security fears for number of reasons. Firstly, customary cryptographic primitives for the purpose of data security protection cannot be directly agreed due to the users' loss control of data under Cloud Computing. Therefore, certification of correct data storage in the cloud must be directed without definite knowledge of the whole data. Bearing in mind various kinds of data for each user stored in the cloud and the demand of long term continuous declaration of their data safety, the problem of authenticating correctness of data storage in the cloud becomes even more challenging.

Secondly, Cloud Computing is not fair a third party data warehouse. The data stored in the cloud may be recurrently modernized by the users, including insertion, modification, appending, deletion, reordering, etc.

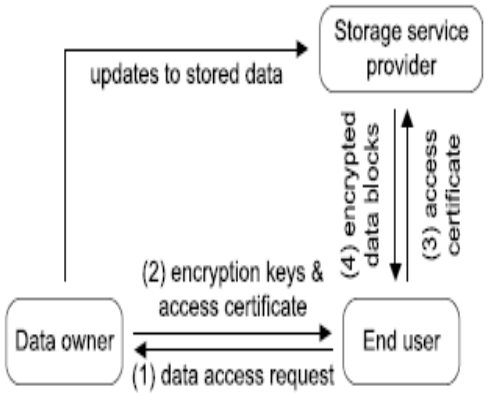

Fig: 2 Cloud Computing Applications

To ensure storage correctness under dynamic data update is hence of utmost importance. On the other hand, this dynamic feature also makes traditional integrity insurance techniques ineffective and demands new solutions.

Last but not the least, the organization of Cloud Computing is powered by data centers running in a synchronized, cooperated and distributed manner. Individual user's data is without cause stored in multiple physical locations to supplementary reduce the data integrity threats.

Accountability is likely to become a fundamental concept in cloud that growth the trust in cloud computing. It helps to suggestion the user's data, shielding sensitive and trusted information, improving user's trust in cloud computing.

2. CLOUD COMPUTING SECURITY

Cloud store the mass amount of users' data, so well-known security is very important. The vendor of the data does not aware about where their data is put in storage and they do not have control of where data is placed.

Here it searches the security experiments in cloud. Some of the security risks consist of secure data transfer, data separation, secure stored data, user access control, and secure software interface. To promote JAR file compression method and security concern of end users accountability mechanism is used.

Here the basic concept is that user's private data are sent to the cloud in an encrypted form, and then with the encrypted data processing is carried out.

3. ACCOUNTABILITY FOR THE CLOUD

Accountability become a fundamental concept in cloud that helps to growth of trust in cloud computing. The term Accountability [1] refers to a contracted and inaccurate requirement that met by reporting and reviewing mechanisms. Accountability is the agreement to act as in authority proctor of the personal information of others, to take accountability for security and applicable use of that information beyond legal requirements, and to be held responsible for misuse of that information.

Forthcoming accountability use preventive controls. Preventive controls for the cloud include risk analysis and policy enforcement, trust assessment, obfuscation techniques, decision support tools, identity management.

Surveying accountability use detective controls. Detective controls for the cloud include reporting, auditing, tracking, and monitoring.

Accountability in cloud motivations on keeping the data usage track able and transparent.

4. RELATED WORKS

4.1 Data storage security in cloud computing

The third party auditor (TPA), who has proficiency and aptitudes that cloud users do not need and is trusted to consider the cloud storage service security on behalf of the user upon invitation. Users depend on the CS for cloud data storage and preservation [19].

They may also enthusiastically interact with the CS to access and update their stored data for various presentation purposes. The users may resort to TPA for make sure the storage security of their outsourced data, while expecting to keep their data private from TPA. We consider the survival of a semi-trusted CS as does. Namely, in most of time it performs properly and does not turn from the agreed protocol execution. However, during provided that the cloud data storage based on the services, for their own benefits the CS might lack of care to keep or purposefully delete rarely accessed data files which belong to conventional cloud users. Moreover, the CS may decide to hide the data exploitations caused by server hacks or Byzantine failures to conserve reputation. We assume the TPA, who is in the business of auditing, is independent and reliable, and thus has no encouragement to plan with either the CS or the users during the auditing process.

TPA should be able to professionally audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users.

IJERT

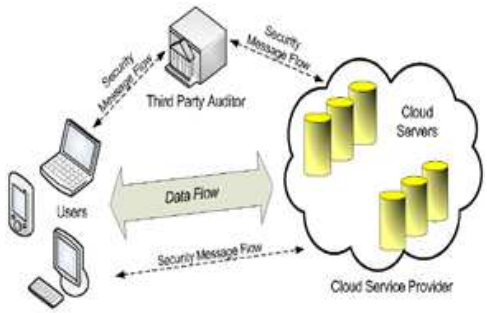

Fig: 3 Architecture cloud storage service

The Cloud Computing model of calculating is a distributed application arrangement that partitions tasks or amount of work between the providers of a resource or service, called Cloud servers.

4.2 Toward publicly auditable secure cloud data storage services

The authors recommend that publicly auditable cloud data storage is able to help this emerging cloud reduced become fully established. Public auditability, a trusted entity with expertise and capabilities data owners do not possess can be passed on as peripheral audit party to assess the risk of contract out data when needed.

Such an reviewing service not only helps save data owners' working out the resources but also provides a transparent up till now cost-effective method for data owners to gain trust in the cloud.

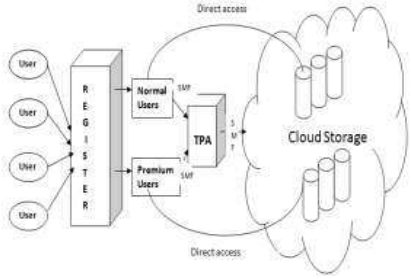

Fig: 4 Architecture of Accountability trust in cloud

The author describe methodologies and system requirements that should be conveyed into consideration, and framework challenges that need to be determined for such a publicly auditable secure cloud storage service to become a authenticity [9].

4.3 Hybrid cloud infrastructure

In the cloud storage has several merits over the cloud data storage. It can be access any location through the internet. So, storing data leakage possible to the cloud service.

Here it is used for the cryptographic approach [15]. In this, trusted data are encrypted and uploaded on cloud from client. It can be responsible for an encryption solution to safeguard files and allow users to view and edit the encrypted file stored in cloud [10].

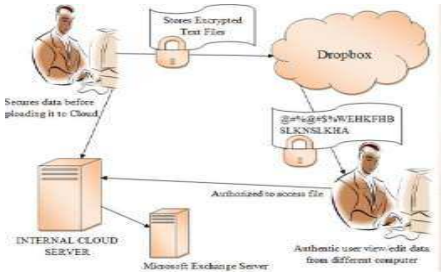

Fig: 5 Design of hybrid cloud infrastructure

Here the public cloud acts as a storage cloud. In the paper use the Drop box that can provide a cloud based service. So, Private cloud is used for the access control, authentication and key management also.

4.4 Multi agent system in the cloud

In the multi agent system techniques provide by the cloud computing security of cloud data storage (CDS) among it. In the architecture offered eleven attributes generated from four main security policies included integrity, correctness, availability and confidentially of the user data in the cloud.

4.5 Proof-carrying code for open environment

Software system used many different computation features and abstraction levels. These will be initial certified systems; it is hard to have a single verification system supportive for all the computation features.

Certified modules (i.e., proof and code) can be linked self-possessed to build fully qualified systems. The framework supports segmental proof and verification reuse. It is also communicative enough so that invariants recognized in specific verification systems are preserved even when they are embedded into our framework [4].

4.6 Elliptic curve cryptography in Data security

In cloud computing, the stored data must be secured. There are many security risks available that include data segregation, data location and recovery etc. Cloud data are usually transmitting between cloud storage and users.

The user doesn't know the particular location where the data are storing. Here authentication and encryption can be providing to the data with elliptic curve cryptography [3]. Elliptic curve cryptography can provide authentication and confidentiality of data between the clouds.

IJERT

Elliptic Curve Cryptography (ECC) is a type of public-key cryptography (PKC) that is based on the algebraic structure of elliptic curves over finite fields. The security of ECC is based on the stiffness of the elliptic curve discrete logarithm badly behaved, and achieves RSA-equivalent security with a much smaller elliptic curve group;

For example, a 163-bit key in ECC is considered to be as secure as 1024-bit key in RSA [16]. ECC putting into practice use less memory and processing power, which allows them to be used on compacted platforms such as smart cards and smart phones.

4.5 Identity based encryption for cloud computing

In the form of public-key cryptography in which use by the third-party server uses a simple identifier, such as the mail-id, to generate the encrypting and decrypting the electronic messages. Associated with typical public-key cryptography, this importantly reduces the difficulty of the encryption method for both administrators and users. In this process, which can be introduced by the sender, a unique identifier of the recipient (such as his mail-id) is used to compute a public key [3].

A trusted third-party server, called for the private-key generator, uses a cryptographic algorithm to analyze the equivalent private key from the public key. In this way, receivers can create their own private keys directly from the server as desirable, and they don't have to concern about allocating their public keys.

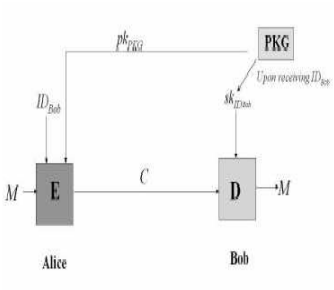

Fig: 6 identity based encryption

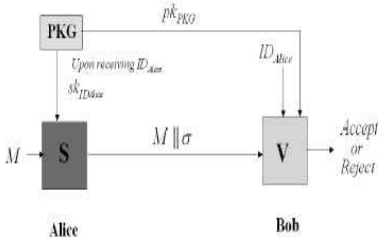

Fig: 7 identity based signature

4.5.1 Pros:

- Keys expire, so they don't need to be revoked. In a traditional public-key system, keys must be revoked if compromised.
- Less vulnerable to spam.
- Enables postdating of messages for future decryption.

4.5.2 Cons:

- Requires a centralized server. IBE's centralized approach implies that some keys must be created and held in escrow and are therefore at greater risk of disclosure.
- Requires a secure channel between a sender or recipient and the IBE server for transmitting the private key.

4.6 Jar files and compression

A JAR (Java ARchive) is a file that contains the image, class and sound files for a java application or applet assembled a single file and feasibly compressed. When a programmer gets a java program development kit, a small program or convenience called “jar” is included.

The jar convenience lets the programmer create, list and extract the individual files from a jar file. They want to keep track their data for knowing whether data is secure or not. Here a framework is used know as Cloud Information Accountability (CIA).

It can provide end to end accountability in distributed approach and also it combines with usage control, access control and authentication.

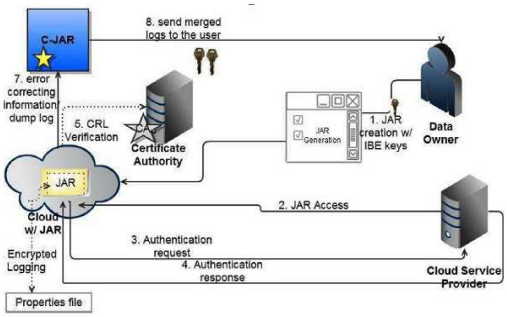

Fig: 8 CIA frameworks

Here Java Archives (JAR) files are used for mechanically log the procedure of the user data. JAR file take account of user’s data and their policies such as right to use control policies and logging policies. By using this framework it helps to growth the trustiness of cloud.

5. EXISTING SYSTEM

Cloud security must be handling with the full care of security. Cloud computing can access the usage control, access control and authentication.

IJERT

Considering the above related works cloud security can be provided by using many methods. Among that the most efficient method is providing by accountability.

So, data awareness also very important in the cloud security. The attacker may assume that the allowing data without noticed by the data owner. Such attacks will be discovered by our auditing mechanism. But it does not enable the data owner to audit even those copies of its data that were made without his knowledge.

6. PROPOSED SYSTEM

In the proposed system security schemes have been implemented to the address of the security issues. It an accessible the JAR file format.

It is automatic created by the log files it contains the (ID, Action, Time, Records id, Signature) log record form. In addition, JAR maintenances compression, which reduces the file size, further improving the download time.

The data also encrypted format. One drawback of the IBE scheme is that heavy workloads are executed on a single PKG. To resolve this problem, a chain of command of PKGs in which the PKGs have to compute private keys only to the entities immediately below them in the hierarchy should be incorporated to a normal IBE scheme [3].

In this hierarchical IBE scheme, which we call a "HIBE" scheme, the users are no longer identified by a single identity [6], as an example, Bob's identity in the HIBE system may be represented as,

(IDBob; IDCompany) = (Bob; cryptworld:com)

This work is tells in general to manageable code transfer, such as java tools, and more particularly to be responsible for security and authentication of manageable code for use by mobile device or other computing devices moderately narrow computing resources and some degree of communication bandwidth.

7. CONCLUSION

In the cloud computing ensure that the trust of cloud from accountability. CIA framework accessible through the JAR files and data also encrypted format by using the Hierarchical identity based encryption.

Similarly to the case of the design and realization of an IBE scheme, could not have a fully functional HIBE scheme. In addition the JAR file can authenticate. So, that it allows the powerful applications too many different mobile devices, information gathering capabilities very high and flexibility.

8. REFERENCE

[1] Andreas Haeberlen,"A case for accountable cloud", Max Planck Institute for Software Systems (MPI-SWS) Cloud Security Alliance (2010) Cloud Audit. The Automated Audit, Assertion, Assessment, and Assurance API) Available: http://cloudaudit.org/

[2] Adi Shamir," Identity-based cryptosystems and signature schemes" In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc.,1985.

[3] Boneh .D and Franklin M.K., "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[4] Feng .X, Ni .Z, Shao .Z, and Guo .X, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.

[5] Gentry .C and Silverberg .A, "Hierarchical ID-Based Cryptography", Proceedings of ASI-ACRYPT 2002, LNCS 2501, Springer-Verlag 2002, pages 548-566.

[6]http://www.crypto.stanford.edu/ibe/download.html

[7] Hess .F, Efficient Identity Based Signature Schemes Based on Pairings, Selected Areas in Cryptography Proceedings of SAC 2002, LNCS 2595, pages 310-324, 2002.

[8] Jagadeesan .R, Jeffrey .A, Pitcher .C, and Riely .J, "Towards a Theory of Accountability and Audit," Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 152-167, 2009.

[9] Jinhui Yao and Chen Wang,"Accountability as a service for data"

[10] Kiruthika .P.M, Amirtha .T and Deepa .M,"Aframework for accountability and trust in cloud computing", International Journal of Communications and Engineering Volume 01NO.1,Issue 03 March 2012.

[11]Mehul A. Shah Ram Swaminathan Mary Baker (2008),"Privacy-Preserving Audit and Extraction of Digital Contents", HP Labs Technical Report No. HPL-32

[12] NTP: The Network Time Protocol, http://www.ntp.org/, 2012.

[13] Open Source Cloud: OpenNebula, http://www.OpenNebula.org/, 2012.

IJERT

[14] Sajithabanu .S and Geogre Prakesh Raj .E ,"Data storage security in cloud ", IJCST vol 2, issue 4, oct dec 2011.

[15] Sonam Chugh and Sateesh Kumar Peddoju, "Access Control Based Data Security in Cloud Computing", Vol. 2, Issue 3, May-Jun 2012, pp.25892593

[16] Sahai .A and Waters .B, "Fuzzy identity based encryption," in Proc. Advances in Cryptology—Eurocrypt , 2005, vol. 3494,LNCS, pp. 457–473.

[17] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi" Data Security in Cloud Computing with Elliptic Curve Cryptography ", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 22312307, Volume-2, Issue-3, July 2012.

[18]www3.ntu.edu.sg/home/ehchua/programming/java/j9d_jar.html

[19] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

IJERT