International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 05
April 2017

Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates

B Mamatha[1]. CH Jayanth[2]. CH Rohit Raj[3]. D Dinesh Reddy[4] B Srikanth Yadav[5]

Assistant 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]

B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[5]

ABSTRACT

Focus on the way to create the key updates as transparent as doable for the consumer and propose a replacement paradigm called cloud storage auditing with verifiable outsourcing of key updates. during this paradigm, key updates is safely outsourced to some licensed party, and therefore the key-update burden on the consumer are going to be unbroken bottom. Specifically, we tend to leverage the third-party auditor (TPA) in several existing public auditing styles, legit play the role of licensed party in our case, and create it in charge of each the storage auditing and also the secure key updates for key-exposure resistance. In our style, TPA solely has to hold Associate in nursing encrypted version of the client's secret key, whereas doing of these burdensome tasks on behalf of the consumer. The consumer solely has to download the encrypted secret key from the TPA once uploading new files to cloud. Besides, our style conjointly equips the consumer with capability to more verify the validity of the encrypted secret keys provided by TPA. of these salient options square measure fastidiously designed to form the complete auditing procedure with key exposure resistance as clear as doable for the consumer.

INTRODUCTION

Cloud storage auditing is used to verify the integrity of the data stored in public cloud, which is one of the important security techniques in cloud storage. In recent years, auditing protocols for cloud storage have attracted much attention and have been researched intensively. Many cloud storage auditing protocols like have been proposed based on this technique. The privacy protection of data is also an important aspect of cloud storage auditing. In order to reduce the computational burden of the client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. However, it is possible for the TPA to get the client's data after it executes the auditing protocol multiple times. Auditing protocols are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic operations. Wang have proposed an auditing protocol supporting fully dynamic data operations including modification, insertion and deletion. Auditing protocols can also

support dynamic data operations.Though many research works about cloud storage auditing have been done in recent years, a critical security problem—the key exposure problem for cloud storage auditing, has remained unexplored in previous researches. While all existing protocols focus on the faults or dishonesty of the cloud, they have overlooked the possible weak sense of security and/or low security settings at the client.

EXISTING SYSTEM

Existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local burdens to the client, especially those with limited computation resources such as mobile phones

EXISTING SYSTEM DISADVANTAGES

Time taken for data load

Data is not secured

PROPOSED SYSTEM

In this paper, we focus on how to reduce the damage of the client's key exposure in cloud storage

e auditing. Many cloud storage auditing protocols have been proposed basedon this technique. The privacy protection of data is alsoan important aspect of cloud storage auditing.

PROPOSED SYSTEM ADVANTAGES

Many auditing protocols for cloud storagehave been proposed to deal with this problem. These protocolsfocus on different aspects of cloud storage auditing suchas the high efficiency , the privacy protection of data, the privacy protection of identities dynamic data operations the data sharing

PROJECT DESCRIPTION

We analyze the problem of unsecure public auditing process in public cloud environment.

PROBLEM DEFINITION

Protocols focus on the faults or dishonesty of the cloud; they have overlooked the possible weak sense of security and/or low security settings at the client.In fact, the client's secret key for cloud storage auditing maybe exposed, even known by the cloud, due to several reasons. Firstly, the key management is a very complex procedure which involves many factors including system policy, user training, etc. One client often needs to manage varieties of keys to complete different security tasks. Any careless mistake or fault in managing these keys would make the key exposure possible.

METHODOLOGIES

Methodologies are the process of analyzing the principles or procedure for enabling secure external auditing process against data integrity and preventing key exposure in public cloud environment.

MODULES

Service Provider

- Authentication
- Resource Provisioning

Third Party Auditor

- Authentication
- Auditing Process

Data Owner

- Authentication

- Key Maker
- Auditing Request

MODULE DESCRIPTION

- **Authentication**

  If you are the new user going to consume the service then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself..

SERVICE PROVIDER

- Resource Provisioning

  The process of providing resources to customers or clients with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts. When used in reference to a client, provisioning can be thought of as a form of customer service.

THIRD PARTY AUDITOR

- Auditing Process

In public auditing module, the auditor perceives and recognizes the propositions before him for examination, collects evidence, evaluates the same and on this basis formulates his judgment which is communicated through his audit report.

DATA OWNER

- Key Maker

In this module, keys are generated according to the user setup in order to generate verification Meta data of uploaded file.

- Auditing Request

User can send the auditing request to external auditor along with the signatures and Meta data of the file. Then auditor will request for generated proof from service provider in order to do auditing process. Finally data owner will get the audit report.

DATA USER

- Access Cloud Data

The authorized data user will get the keys from the data owner and access their data from the cloud environment.

ALGORITHM USED

Blinding

Blinding technique with homomorphic property to form the encryption algorithm to encrypt the secret keys held by the TPA. It makes our protocol secure and the decryption operation efficient. Meanwhile, theTPA can complete key updates under the encrypted state.**The Algorithm Steps**

In the Lazy update techniques process is as follows:

Step 1: SysSetup(usually at random)

Step 2: Until "done"

- Key Update
- Authentication Generation
- Proof Gen
- Proof Verify

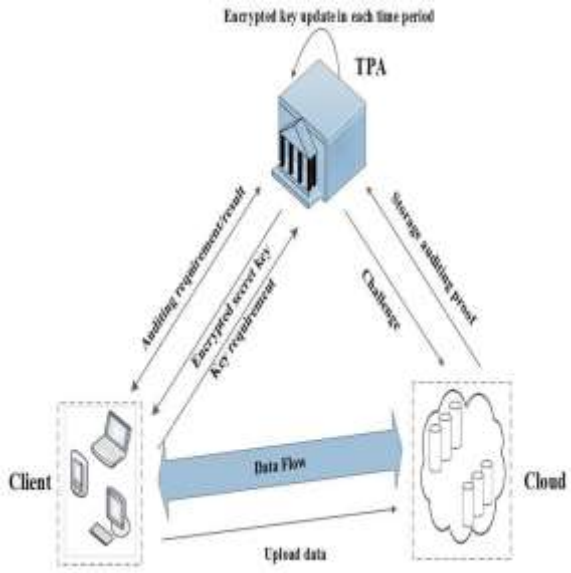
Step 3: Repeat

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.

SYSTEM ARCHITECTURE

The users or nodes involved in our projects are Sender, Intermediate and Receiver. In order to send file, the sender has to find out the list of nodes which are connected with the sender. From that available list he can choose receiver. Then the sender has to analyze the performance of each and every node which is connected with the sender. The performance analysis list will return the priority based result so that sender can choose the intermediate to send the file. The Intermediate will receive the file from sender then it will analyze the performance so that it can send data to another intermediate or receiver. In the receiver side, the receiver has to select the file path to receive the file from sender or intermediate. Then the receiver can view the file received file.



INTRODUCTION TO DOTNET

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. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.

".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).

ASP.NET OVERVIEW

ASP.Net is a web development platform, which provides a programming model, a comprehensive software infrastructure and various services required to build up robust web application for PC, as well as mobile devices.

ASP.Net works on top of the HTTP protocol and uses the HTTP commands and policies to set a browser-to-server two-way communication and cooperation.

ASP.Net is a part of Microsoft .Net platform. ASP.Net applications are complied codes, written using the extensible and reusable components or objects present in .Net framework. These codes can use the entire hierarchy of classes in .Net framework.

SQL SERVER 2008

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.

Improvements to the database engine, the details of which are not published by Microsoft, and the corresponding changes to the main infrastructure components are reflected by a substantial number of new features as well as enhancements to existing ones. The most relevant ones can be grouped into several categories, such as high availability and scalability, security, data management, administration and maintenance, and development.

CONCLUSION

In such a protocol, the integrity of the data previously stored in cloud can still be verified even if the client's current secret key for cloud storage auditing is exposed. We formalize the definition and the security model of auditing protocol with key-exposure resilience, and then propose the first practical solution. The security proof and the asymptotic performance evaluation show that the proposed protocol is secure and efficient

REFERENCES

[1] G. Attendees et al., "Provable data possession at untrusted stores, "in Proc. 14th ACM Conf. Compute. Common.Secure., 2007,pp. 598–609.

[2] G. Ateniese, R. Di Petro, L. V. Mancini, and G. Tsudik, "Scalable andefficient provable data possession," in Proc. 4th Int. Conf. Secure.PrivacyCommon.Newt., 2008, Art. ID 9.

[3] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, andJ.-J. Quisquater, "Efficient remote data possession checking in critical information

infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20,no. 8, pp. 1034–1038, Aug. 2008

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multipleeplicaprovable data possession," in Proc. 28th IEEE Int. Conf. Distrib.Comput. Syst., Jun. 2008, pp. 411–420

[5] H. Shacham and B. Waters, "Compact proofs of retrievability,"in Advances in Cryptology—ASIACRYPT. Berlin, Germany:Springer-Verlag, 2008, pp. 90–107.

[6] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24,Jul./Aug. 2010.

[7] Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S. S. Yau, "Efficientprovable data possession for hybrid clouds," in Proc. 17th ACM Conf.Comput.Commun.Secur., 2010, pp. 756–758.

[8] K. Yang and X. Jia, "Data storage auditing service in cloud computing:Challenges, methods and opportunities," World Wide Web, vol. 15, no. 4,pp. 409–428, 2012.

[9] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocolfor data storage in cloud computing," IEEE Trans. Parallel Distrib.Syst.,vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[10] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreservingpublic auditing for secure cloud storage," IEEE Trans.Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.