ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Trusted Cloud for Data Sharing

Vishal V.Bhanawase[*1], Shweta S.Umbarje[2], Ashwini A. Bagale[3], Ashwini B.Karimungi[4]
[*1,2,3,4] V.V.P.I.E.T.,Solapur, Maharashtra, India
vishal1234_2@yahoo.com

Abstract

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a Service (PaaS) and Software-as-a-Service (SaaS). A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic - a user can have as much or as little of a service as they want at any given time and the service is fully managed by the cloud service provider (the consumer needs nothing but a personal computer and Internet access).The advantage of cloud is cost savings. The prime disadvantage is security. Cloud computing is used by many software industries nowadays. Since the data placed in the cloud is accessible to everyone, security is not guaranteed. Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites. Since Cloud Computing share distributed resources via network in the open environment thus it makes security problems. All types of users who require the secure transmission or storage of data in any kind of media or network. By this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services. To allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud.

Keywords: Cloud computing, accountability, Privacy, auditing, data sharing, security.

Introduction

The main concept behind cloud computing is here computing is done in remote location. Basically it is done in a virtualization environment implemented on large servers. Cloud computing gives new way of hosting and processing of data by providing scalable and often virtualized resources. Now days there are many commercial cloud service providers are offering service including Amazon, Google, Microsoft, Yahoo and Sales force etc. The main advantage behind the success of this technology is that anyone can use this technology for those users don't need to be expertise of that technology infrastructure. While enjoying the facility brought by this emerging technology user also started worrying about the fate of their data as they don't know in which machine their data is stored and who is processing their data. This worry has raised so many security issues and it is a known fact that only SLA's (service level agreement) can't give desired security to the user's data. Cloud is a layered architecture where user data is processed by so many service providers and it is highly impossible for the user to track their data.

Existing System

To allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments.

Problems in existing system

First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on.

ISSN: 2277-9655
Impact Factor: 1.852

Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

Although the Cloud computing is vast developing technology, the database management system does not have a trustworthiness

Proposed System

To overcome the above problems, we propose a novel method, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Data Owner can upload the data into the cloud server after encrypted the data. User can subscribe into the cloud server with certain access polices such as read, write and copy of the original data. The Loggers and Log Harmonizer will have a track of the access logs and reports to the data owner. This Process ensures security.

Advantage

We can share the data in a secured manner and another advantage is particular user is access data as access permission.

Cloud Service Provider

A Cloud Service Provider (CSP) who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

In this paper, CIA (Cloud Information Accountability) framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Distinct modes for auditing are push mode and pull mode.

Modification

If any user is download file on cloud server then that user is called user and if that user is upload any file on the cloud server then that user called as a data owner for that particular file.

The part is administrator that monitoring all things in cloud. If any illegal action or misuse of data in cloud performed by the user then administrator has priority to delete that data and also user's access priorities are removed by the administrator. In this way administrator detecting the misuse or illegal operation in cloud but not preventing all these things.

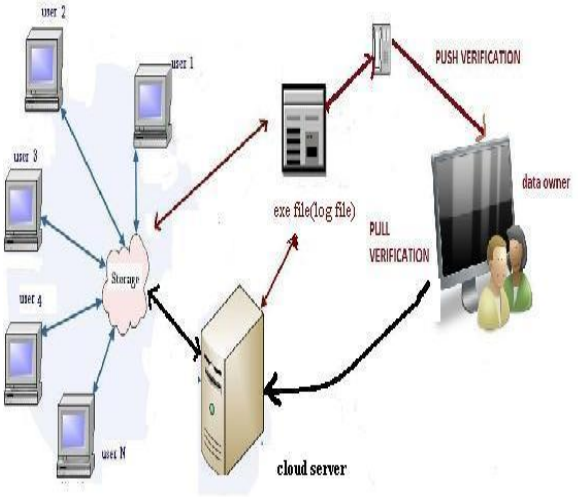

Fig: Overall Structure

Modules

- User
- Data Owner
- Cloud Sever
- Logger
- Access Privileges
- Push And Pull
- Random Set Generation And Verification

User

User is the person is going to view or download the data from the Cloud server. To access the data from the Cloud server, the users have to be registered with the cloud server. So that the user have to register their details like username, password, security question answer and a debit card number to pay the amount to cloud server. This is the information that will store in the database for the future authentication. And also users are categorized into three ways first silver that user will only view or download the text files.second gold user these users are access text files with image files. And third user is platinum this user access all files in cloud. they are pay the amount as per user type.

ISSN: 2277-9655
Impact Factor: 1.852

Data Owner

Data Owner is the Person who is going to upload the data in the Cloud Server. In order to upload the data into the Cloud server, the Data Owner have to be registered in the Cloud Server. Once the Data Owner registered in cloud server, the space will be assigned to the Data Owner. Cloud Server is the area where the user going to request the data and also the data owner will upload their data. Once the user send the request regarding the data they want, the request will first send to the Cloud Server and the Cloud Server will forward your request to the data owner. The data Owner will send the data to the user via Cloud Server. The Cloud Server will also manage the Data owner and Users information in their Database for future purpose.

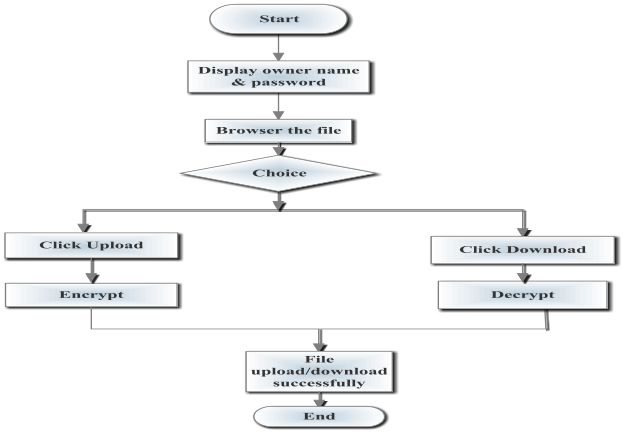

Figure: User Module

Logger

The Logger is maintained by the Cloud Server. Loggers have the details of the data owner and users who are accessing the Cloud Server. So the Logger will be more useful for many purposes. Like which user / data owner accessing the Cloud Server, accessed at the particular time, which file is access and the IP address from which the data is requested by user etc.

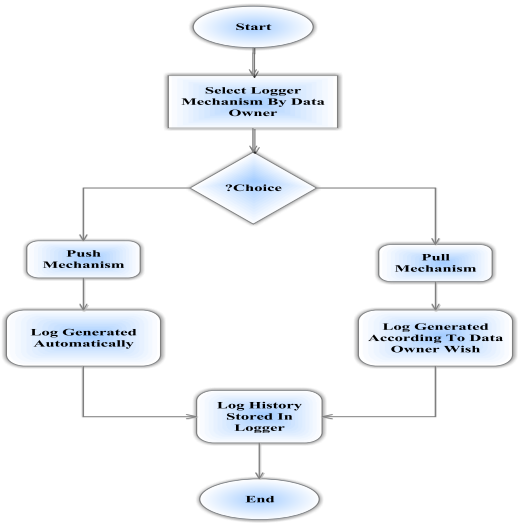

Figure: Control Module for Logger

Access Privileges

The access privileges are set by the data owner for accessing their data. Some Owners will provide read only, some of them will allow read and download. The Cloud Server will send the dynamic intimation when the user is accessing the data beyond their limits. This increases more security while sharing the data in the Cloud.

Push and Pull Concept

Push

For the every periodical time the Cloud Server will send the access details of the user to the data owner. So that the Data Owner may able to know who're all the accessing their data at the particular time period. During the registration phase, the Data owner will ask by the Cloud Server whether they're choosing the push or pull method

Pull

In the Pull method, the data owner has to send the request to the Cloud Server regarding the access details of their data up to the particular time. Then the Cloud Server will send the response to the Data Owner regarding the user's access details.

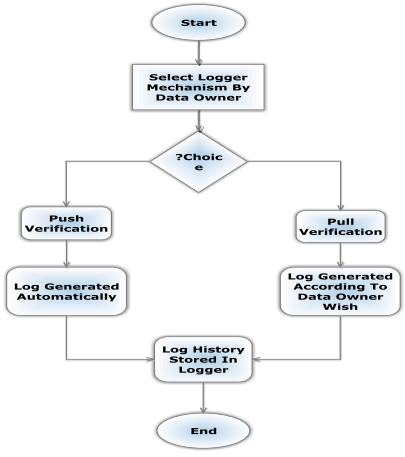

Figure: Push and Pull Verification

Transaction password and Verification

When the user request the data to be downloaded from the Cloud Server, the user have to enter the transaction. If it is matched, the user is allowed to download the data. The transaction

ISSN: 2277-9655
Impact Factor: 1.852

password will be entered by the user during the registration Phase itself. This ensures security while downloading the data.

Implementation

Technology Overview

A] .NET

.Net is a software framework developed by Microsoft that runs primarily on Microsoft windows. It includes large library and provides language interoperability (each language can use code written in other languages)across several programming languages .Programs written for .Net framework execute in a software environment known as the Common Language Runtime(CLR),an application virtual machine that provides services such as security, memory management and exception handling.

B] ASP.NET

ASP.NET is a server -side web application framework designed for web development to produce dynamic web pages .It was developed by Microsoft to allow programmers to build dynamic web sites, web applications and web services. It was first released in January 2002 with version 1.0 of the .NET framework, and is the successor to Microsoft's Active Server Pages(ASP) technology.ASP.NET is built on the Common Language Runtime(CLR),allowing programmers to write ASP.NET code using any supported .NET language. The ASP.NET SOAP extension framework allows ASP.NET components to process SOAP messages.

C] Interface with Cloud Server

In implementation, user can search, download and upload any file on cloud server. User register to cloud server then create space on cloud server to that user.

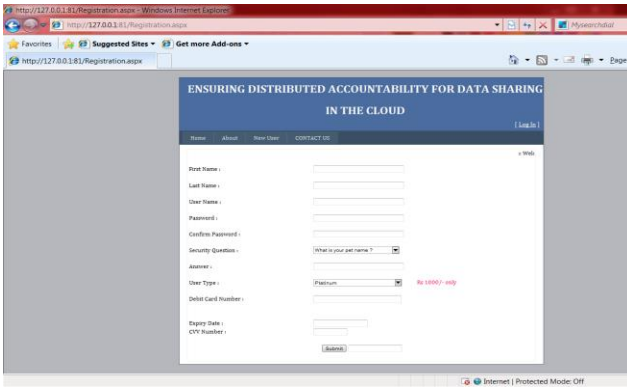

Fig: Registration form

In this figure user and data owner are registration to cloud server. And all information stored on cloud server that is log's are maintained.

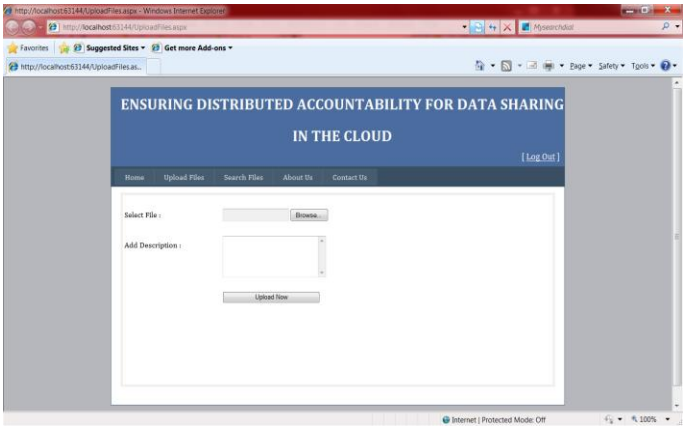

Fig: Searching Form

In This figure user can searching of data on cloud example audio, video and text files using file name or file description or either file extension

Conclusion

The innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism are proposed. This approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge. This research is aimed at providing software tamper resistance to our applications. In the long term, it will be planned to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of traveling content. A variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls would be supported.

Future Enhancement

To verify the integrity and the authentication of log files Without decrypting the file by the data owner, can check the log files. To support a variety of security policies, like indexing policies for text files, usage control for executables

References

[1] *Pankaj Kumar,Singh Ajit Kumar,R.Karthikeyan, "Ensuring Distributed Accountability for Data Sharing in the Cloud" , International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 3, March 2013*

[2] *"Improvising Distributed Accountability by Using Fog Methodology",International*

Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-6, August 2013

[3] *E. Barka and A. Lakas, "Integrating Usage Control with SIP-BasedCommunications," J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.*

[4] *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.*

[5] *P.T. jaeger,J.Lin,and J.M.grimes, "cloud computing and information policy," pp 2006.*

[6] *R. Bose and J. Frew, "Towards a theory of accountability and audit," vol. 37, pp. 1- 28, Mar. 2005.*

[7] *P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '06), pp. 539-550, 2006.*

[8] *B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf.System Sciences (HICSS), 2004.*

[9] *R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.*

[10] *B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001*

[11] *Y. Chen et al., "Oblivious Hashing: A Stealthy SoftwareIntegrity Verification Primitive," Proc. Int'l Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.*

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