International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Optimizing the Cloud Multimedia Resources using Attribute Based Access through Virtualization

Patil Siddharam[1], **Rekha Patil**[2]

[1]M. Tech, Department of Computer Science and Engineering, Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

[2]Associate Professor and HOD, Department of Computer Science and Engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

Abstract: ***Cloud Computing has been envisioned as the emerging technology in which resources are provided as services over the Internet. When there is large number of users, it is difficult to check the data integrity, confidentially between user and Cloud Service Provider (CSP). In such scenarios, Third Party Auditor (TPA) is employed who not only manages the data but also intimates the user if data modified. When users outsource data to un-trusted servers, existing systems usually apply cryptographic techniques by allowing only authorized user to access the contents .This inevitably introduces computation overhead on data owner. In order to overcome this, proposed scheme defines a way to access the data based on access policy which is defined by data owner.***

Keywords: Cloud Computing, Cryptographic Techniques, Third Party Auditor, Attribute Based Access.

1. Introduction

The Internet is an electronic communication network that connects computer networks and organizational computer facilities around the world. It is publicly accessible computer network connecting many smaller networks from around the world. Cloud computing is one of the technology that uses internet to delivers many types of resources. Therefore, cloud computing can be identified as a technology that uses the Internet as the communication medium to deliver its services. Cloud computing alludes to applications and services that run on a distributed system utilizing virtualized resources based upon internet protocols and networking principles. The use of word "cloud" makes reference to the two essential concepts:

- Abstraction: Cloud computing abstracts the details of system implementation from users and developers. Applications run on physical systems that are not specified, data stored in location that are unknown, administration of systems outsourced to others , and access by users is ubiquitous.
- Virtualization: Cloud computing virtualizes systems by polling and sharing resources. Systems and storage can be provisioned as needed from a centralized infrastructure, costs are assessed on metered bases, multi-tenancy is enabled, and resources are scalable with agility.

To have the complete overview of cloud computing, one needs to define the lexicon of cloud computing. Cloud computing separated into two distinct set of models:

- **Deployment models**: These refer to location and management of the cloud's infrastructure.
- **Service models**: These consist of particular types of services that users can access on a cloud computing platform.

1.1 Deployment Models of Cloud Computing

A deployment model [1] defines the purpose of the cloud and the nature of how the cloud is located.

1.1.1 Public Cloud

Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure. Generally, public cloud providers like Amazon AWS, Microsoft and Google own, operate the infrastructure and offer access over the Internet. With this model, customers have no visibility or control over where the infrastructure is located. It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances. Public cloud customers benefit from economies of scale, because infrastructure costs are spread across all users, allowing each individual client to operate on a low-cost, “pay-as-you-go” model. Another advantage of public cloud infrastructures is that they are typically larger in scale than an in-house enterprise cloud, which provides clients with seamless, on-demand scalability. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds.

A public cloud is the obvious choice when:

- Standardized workload for applications is used by lots of people, such as e-mail.
- There is need to test and develop application code.
- There is need for incremental capacity (the ability to add compute resources for peak times).
- For collaboration projects.

1.1.2 Private Cloud

Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. It is not shared with other organizations, whether managed internally or by a third-party, and it can be hosted internally or externally.

There are two variations of private clouds:

1) **On-Premise Private Cloud**: This type of cloud is hosted within an organizations own facility. A businesses IT department would incur the capital and operational costs

Licensed Under Creative Commons Attribution CC BY

for the physical resources with this model. On-Premise private clouds are best used for applications that require complete control and configurability of the infrastructure and security.

2) **Externally Hosted Private Cloud**: Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. The service provider facilitates an exclusive cloud environment with full guarantee of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources.

Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment and it will require the organization to reevaluate decisions about existing resources. Private clouds are more expensive but also more secure when compared to public clouds. An Info-Tech survey shows that 76% of IT decision-makers will focus exclusively on the private cloud, as these clouds offer the greatest level of security and control.

A private cloud is the obvious choice when:

- There is need for data sovereignty with cloud efficiencies
- There is need for consistency across services
- Data center must become more efficient
- There is provision of private cloud services

1.1.3 Hybrid Cloud

Hybrid clouds are composed of two or more clouds (private or public) that remain as unique entities but are bound together offering the advantages of multiple deployment models. In a hybrid cloud, one can leverage third party cloud providers in either a full or partial manner; increasing the flexibility of computing. Augmenting a traditional private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Hybrid cloud architecture requires both on-premise resources and off-site server based cloud infrastructure. By spreading things out over a hybrid cloud, one should keep each aspect of their business in the most efficient environment possible. The downside is that one should keep track of multiple cloud security platforms and ensure that all aspects of business can communicate with each other.

Here are a couple of situations where a hybrid environment is best:

- If company wants to use a SaaS application but is concerned about security.
- If company offers services that are tailored for different vertical markets. One can use a public cloud to interact with the clients but keep their data secured within a private cloud.
- If there is a provision of public cloud to customers while using a private cloud for internal IT.

1.1.4 Community Cloud

A community cloud is a multi-tenant cloud service model that is shared among several organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider. Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group. These communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives. The goal of community clouds is to have participating organizations realize the benefits of a public cloud with the added level of privacy, security, and policy compliance usually associated with a private cloud. Community clouds can be either on-premise or off-premise. Here are a couple of situations where a community cloud environment is best:

- Government organizations within a state that need to share resources.
- A private Health Insurance Portability and Accountability Act (HIPAA) compliant cloud for a group of hospitals or clinics.

1.2 Service Models

In the deployment model, different cloud types are an expression of the manner in which infrastructure is deployed. One can think of the cloud as the boundary between where client's network, management, and responsibilities ends and cloud service providers begins. As cloud computing has developed, different vendors offer clouds that have different services associated with them. The portfolio of services offered adds another set of definitions called service model [2].

1.2.1 Software-as-a-Service (SaaS)

SaaS provides complete applications to a cloud's end user. It is mainly accessed through a web portal and service oriented architectures based on web service technologies as shown in Fig 1.1. Credit card or bank account details must be provided to enable the fees for the use of the services to be billed.

The main differences between the services on the application layer and the classic ASP model are the encapsulation of the application as a service, the dynamic procurement, and billing by units of consumption (pay as you go). However, both models pursue the goal of focusing on core competencies by outsourcing applications.

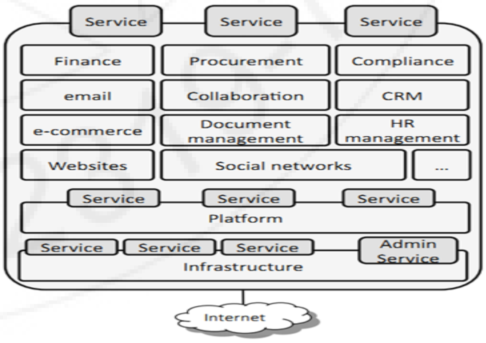


Figure 1.1: Software-as-a-Service

1.2.2 Platform-as-a-Service (PaaS)

PaaS comprises the environment for developing and provisioning cloud applications. The principal users of this layer are developers seeking to develop and run a cloud application for a particular platform. They are supported by the platform operators with an open or proprietary language, a set of essential basic services to facilitate communication.

Licensed Under Creative Commons Attribution CC BY

They are also supported by, monitoring, or service billing, and various other components, for instance to facilitate startup or ensure an application's scalability and/or elasticity (see figure 1.2). Distributing the application to the underlying infrastructure is normally the responsibility of the cloud platform operator. The services offered on a cloud platform tend to represent a compromise between complexity and flexibility that allows applications to be implemented quickly and loaded in the cloud without much configuration. Restrictions regarding the programming languages supported, the programming model, the ability to access resources, and persistency are possible downsides.

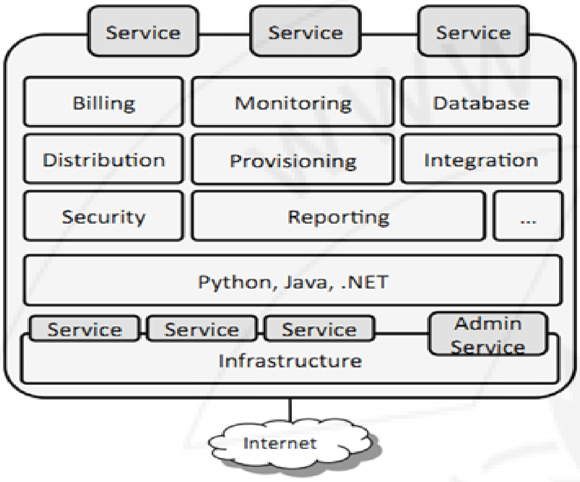


Figure 1.2: Platform-as-a-Service

1.2.3 Infrastructure-as-a-Service (IaaS)

The services on the infrastructure layer are used to access essential IT resources that are combined under the heading Infrastructure-as-a-Service (IaaS). These essential IT resources include services linked to computing resources, data storage resources, and the communications channel. They enable existing applications to be provisioned on cloud resources and new services implemented on the higher layers. Physical resources are abstracted by virtualization, which means they can then be shared by several operating systems and end user environments on the virtual resources – ideally, without any mutual interference. These virtualized resources usually comprise CPU and RAM, data storage resources (elastic block store and databases), and network resources as shown in Fig 1.3.

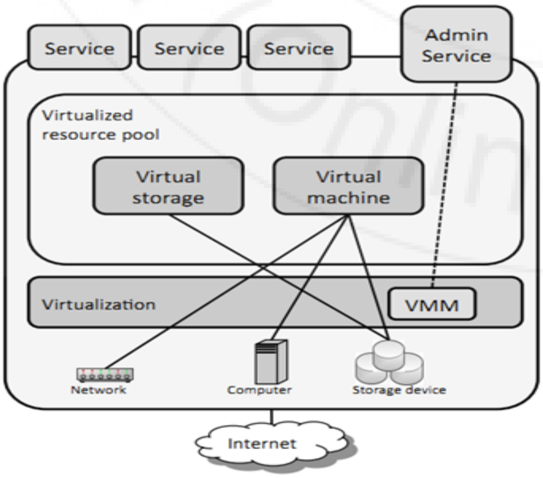


Figure 1.3: Infrastructure-as-a-Service

1.3 Characteristics of Cloud

- On-demand self-service: A client can provision computer resources without the need for interaction with cloud service provider personnel.
- Broad networks access: Access to resources in cloud is available over the network using standard methods in a manner that provides a platform-independent access to clients of all types.
- Resources pooling: A cloud service provider creates resources that are pooled together in a system that supports multi-tenant usage.
- Rapid Elasticity: Resources can be rapidly and elastically provisioned.
- Measured Service: Resources are measured, audited, and reported to the customer based on metered system.

2. Motivation

Existing schemes aim at providing integrity verification for different data storage systems but these systems do not deal with supporting both public audibility and data dynamics. In the proposed approach, on the behalf of cloud client, TPA is used to verify the integrity of dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether data stored in cloud is indeed intact, which can be important in achieving good economies of scale for Cloud Computing.

With this, proposed scheme also endeavor to implement fine-grained data access control in which each data file can be associated with a set of attributes which are meaningful in the context of interest. The access structure of each user can thus be defined as a unique logical expression over these attributes to reflect the scope of data files that the user is allowed to access. As the logical expression can represent any desired data file set, fine-grained of data access control is achieved. To enforce these access structures, it is necessary to define a public key component for each attribute. Data files are encrypted using public key components corresponding to their attributes. User secret keys are defined to reflect their access structures so that a user is able to decrypt a ciphertext if and only if the data file attributes satisfy access structure.

3. System Analysis and Requirements Specification

3.1 System Analysis

In this section, the problem definition and details of proposed system will be discussed.

3.1.1 Problem Definition

Proposed scheme provides a mechanism for data integrity and for confidentiality. In this scheme, CSP provides service, where user is authenticated by CSP and provides a Virtual Machine (VM) by means of Software as a service. If user acts as data owner then while uploading a file, data owner will encrypt the file using RSA algorithm which exists in VM. SHA-1 algorithms also defined in the VM which create the message digest. This message digest is a combination of client encrypted file, digital signature and mode of operation i.e. updating of records or insertion of records or deletion of records and for retrieval for data by users (receiver), TPA uses matrix based method to check the integrity between CSP and user (receiver). And also in this, system uses fine-grained access structure to allow users to access the files based on access policy where, TPA maintains secret key for every file and client can access the file by requesting to TPA.

3.1.2 Proposed System

- This proposed scheme defines a way to implement Third Party Auditor (TPA) who not only manage the data but also tells the client that how much CSP is reliable and keeps the data safe.
- In this system, TPA provides a transparent and cost-effective approach for establishing trust between users and cloud service provider. Based on the audit report of TPA, the released audit result would help the data owner to evaluate the risk of their subscribed cloud data services, and also beneficial for the CSP to improve their cloud based service platform.
- To the best of our knowledge, system simultaneously achieves fine-grainedness, scalability and data confidentiality for data access control in cloud computing.
- The proposed scheme enables the data owner to delegate most of computation intensive tasks to cloud servers without disclosing data contents or user access privilege information;
- The proposed scheme is provably secure under the standard security model. In addition, proposed scheme is able to provide security for multimedia resources.

4. System Design

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. It could be seen as the application of system theory to product development.

4.1 System Architecture

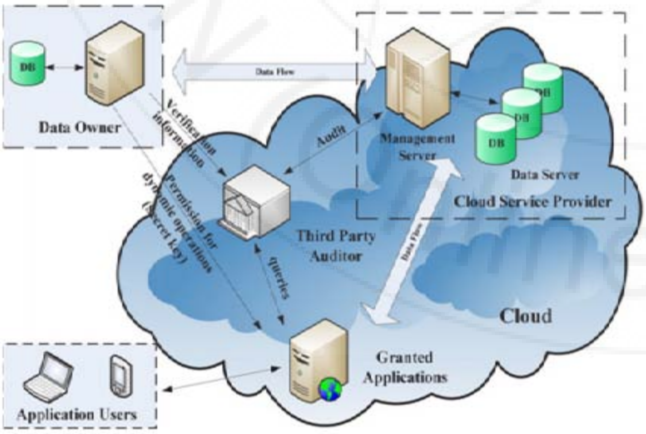


Figure 4.1: System Architecture

As shown in above fig 3.1, CSP provides service, where user is authenticated by CSP and CSP provides a VM by means of Software as a service. If user acts as data owner then while uploading a file data owner will encrypt the file using RSA algorithm which exists in Virtual Machine. SHA-1 algorithms also defined in VM which create the message digest. This message digest is a combination of client encrypted file, digital signature and mode of operation i.e. updating of records or insertion of records or deletion of records and for retrieval of data by users (receiver), TPA uses matrix based method to check the integrity between CSP and user (receiver). And also in this, system uses fine-grained access structure to allow clients to access the files based on access policy where TPA maintains secret key for every file and client can access the file by requesting to TPA.

4.2 Data Flow Diagram

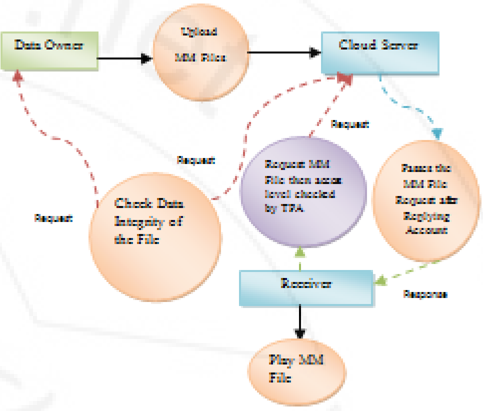

Data Owner
Upload MM Files
Cloud Server
Request
Request
Request
Check Data Integrity of the File
Request MM File then acces level checked by TPA
Passes the MM File Request after Replying Account
Receiver
Response
Play MM File

Figure 4.2: Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. DFDs can also be used for the visualization of data processing (structured design).On a DFD, data items flow from an external data source or an internal data store to an internal data store or an external data sink, via an internal process. A DFD provides no information about the timing of processes, or about whether processes will operate in sequence or in parallel. In this, data owner uploads the file onto cloud where the authenticated user can download the files which lies in user's access level by requesting for secret key to TPA. If the file is not lies in user's access level then TPA will denies for accessing the data.

Licensed Under Creative Commons Attribution CC BY

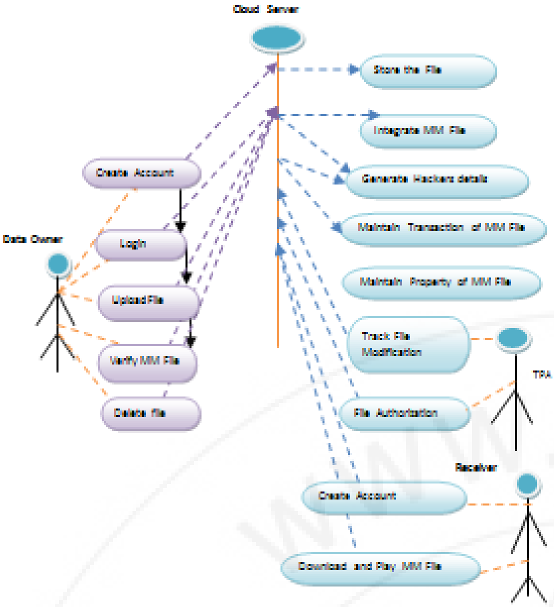


Figure 4.3: Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show relation between functions of systems and roles of actors. A use case diagram is a type of behavioral diagram created from a Use-case analysis. As shown in figure 4.3, user create an account by registering into cloud in which user is authenticated at login time by CSP. After login, if any user uploads the file onto cloud then, user acts as data owner for that file. TPA will maintain the property of a file by checking the integrity of file. If anyone modifies the file TPA intimate to data owner. In receiver side, if any user wants to access the files which are lies in respective user's access level then user will first authenticated by CSP. After that, user can download the file by requesting to TPA, in which TPA maintains secret keys for files.

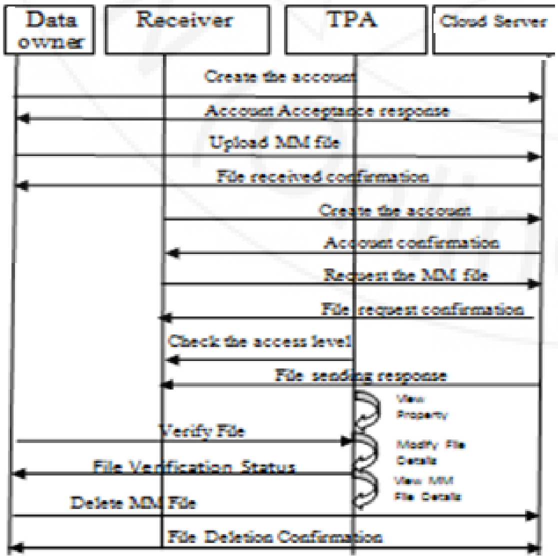


Figure 4.4: Sequence Diagram

As shown in sequence diagram, parallel vertical lines shows different processes or objects that live simultaneously, horizontal arrows shows the messages exchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.UML sequence diagrams model the flow of logic within the system in a visual manner, enabling both to document and validate the logic. As shown in above figure, users create an account by registering into cloud in which users are authenticated at login time by CSP. After login, any user acts as Data owner, if he uploads the file into cloud in which it is stored in CSP. TPA will maintain the property of a file by checking the integrity of file. If anyone modifies the file TPA intimate to data owner. If data owner wants to delete the file then he can delete it. In receiver side, if any user wants to access files which are lies in user's access level then user will first authenticated by CSP. After that, user can download the file by requesting to TPA, in which TPA maintains secret keys for files.

5. Implementation Details

In this section, the implementation details of the proposed system involving distinct modules are discussed.

1. Registration
2. Data integrity check mechanism
3. Data privacy mechanism
4. Accessing the data based on access policy

5.1 Implementation Description

5.1.1 Registration

Users first register into cloud to make utilization of resources which are accessible in cloud through registration module. After that users again login to make utilization of resources which are accessible in cloud. In registration stage based upon users attributes, users will be operated at specific access level. Each user in cloud in some cases acts as data owner or data receiver. In the event that any user needs to transfer the data onto cloud then user goes about as data owner for that data in which, if data owner wants to verify the data then, data owner can confirm by checking data integrity by asking to TPA. If any user wants the data which is in cloud then user will be authenticated by CSP in which, user can access the data only if data lies in user's access level.

5.1.2 Data Integrity Check Mechanism

1. Integrity checks mechanism between Data owner and CSP:

Sometime happens that data send by users or data owner are not correct or transmission error or any error then who will accounts for data. To ensure that data reach to a CSP is in correct form and also send by the authenticate user, proposed system uses new scheme. In this scheme encrypted form of message (F') will be used for message digest along with digital signature of user. This message digest will be made with SHA-1 algorithm. Digital signature is symbol of user's or data owner identity. In case of failure at user or data owner side, digital signature will resolve the problem of accountability. Message digest will helps in ensuring integrity of data. After getting message digest it will be merged with encrypted form of message which results in T_d

Licensed Under Creative Commons Attribution CC BY

i.e. data. This data is send to CSP where first it disintegrate the data form T_d to encrypted message (F‘) and message digest uses SHA-1 algorithms to check (F‘) with (F‘) came from message digest and also check the identity of data owner. If it find something wrong in file then it will ask the user or data owner to send the file again or if it's correct then it update this file according to this instruction is in message digest.

2. Integrity checks mechanism between Receiver and TPA.

Considering the large size of the outsourced data and the owner‘s constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. Hence, to fully ensure data security and save data owner’s computation resources, proposed scheme enables the publicly auditable cloud storage services, where data owners can resort to an external TPA to verify the outsourced data when needed. Third party auditing provides a transparent and cost-effective approach for establishing trust between user and cloud service provider. In fact, based on the audit report of TPA, the released audit result would help data owner to evaluate the risk of their subscribed cloud data services, and also beneficial for the CSP to improve their cloud based service platform.

First data owner or user converts the content of file into ascii value and organize the digit in n*n matrix in such a way that whenever space encountered, it value will be written in matrix as 0. Let A be the matrix. After that system will find inverse matrix of A i.e.$A^{\square 1}$.

Now at Receiver side, numeric key provided by TPA to Receiver is T_{k1} and information that system going to store in Meta date of file is $M_{i.}$.

Now TPA also calculates the value of M_i and compares the value with previous value of M_i. If M_i is equal to previous M_i then report the receiver that CSP is reliable and safe.

5.1.3 Data Privacy Mechanism and Access Mechanism

Data privacy protection are always a concerning factor for owner. Thus, the implementation of protocol should not violate the privacy of owner‘s data. In other words a TPA should be able to efficiently audit the cloud data storage and also TPA should not understand the data. So clients after performing file operation, it will send the data to CSP and TPA. This server and TPA will keep data not only safe but also provide integrity but, how data owner will trust on TPA, if TPA and CSP can send data owner‘s data to unauthorized user. Even removal of TPA will not solve the problem because CSP can also send the data to unauthorized user and also data owner does not get an advantage of TPA. So cryptography is required at user level.

System Setup: In this operation, the data owner chooses a security parameter k and calls the algorithm level interface setup (k) which outputs the system public parameter PK and the system master key MK. The data owner then signs each component of PK and sends PK along with these signatures to cloud servers.

New File Creation: Before uploading a file to cloud servers, the data owner processes the data file as follows.

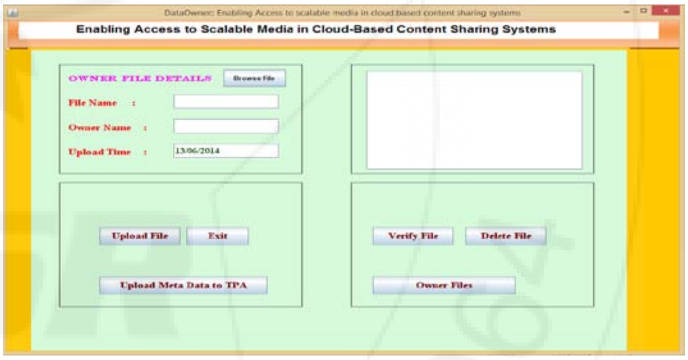
- Select a unique *ID* for this data file;
- Randomly select a symmetric data encryption key DEK ← K, where k is the key space and encrypt the data file using DEK;
- Define a set of attribute I for the data file and encrypt DEK with I using key policy.
- Finally, each data file is stored on the cloud; in which TPA generate a key for every file.

New User Grant: When a new user wants to join the system, the data owner assigns an access structure and the corresponding secret key to this user as follows.

- Assign the new user a unique identity w and an access structure P
- Generate a secret key SK for w.
- With secret key user can access a file which lies in respective user’s access level by requesting to TPA.

File Deletion: This operation can only be performed at the request of the data owner. To delete a file, the data owner sends the file’s unique ID along with data owner’s signature on this ID to Cloud Servers. If verification of the owner’s signature returns true, cloud servers delete the data file.

6. Results



DataOwner: Enabling Access to scalable media in cloud based content sharing systems

Enabling Access to Scalable Media in Cloud-Based Content Sharing Systems

OWNER FILE DETAILS

File Name :

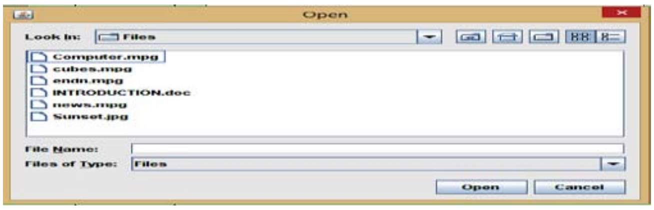
Owner Name :

Upload Time : 13/06/2014

Figure 6.1: Data owner home page

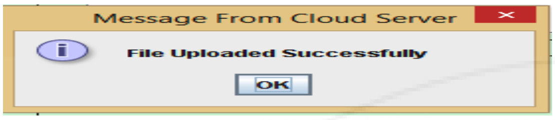
As shown in figures 6.1-6.8, authorized data owner uploads the file to cloud server in which first data owner browse the files for uploading. After browsing, data owner selects the file which data owner wants to upload. After uploading the file, data owner will get the response as “File uploaded successfully”. After uploading the file to CSP, data owner will send metadata to TPA in which it encompasses of file details. After uploading metadata, if data owner wants to verify whether the file is safe or not in cloud server then, data owner will verify for uploaded file. If file is safe then, data owner will get the message as “your file is safe”. If someone modified the file in the middle, then data owner will get the message as “your file is not safe!!It is modified”.

Licensed Under Creative Commons Attribution CC BY



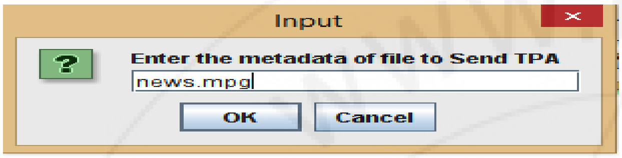
Computer.mpg
cubes.mpg
endn.mpg
INTRODUCTION.doc
news.mpg
Sunset.jpg

Figure 6.2: Browsing the files



File Uploaded Successfully

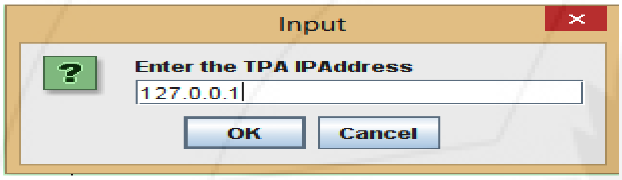
Figure 6.3: Message after uploading



Enter the metadata of file to Send TPA

news.mpg

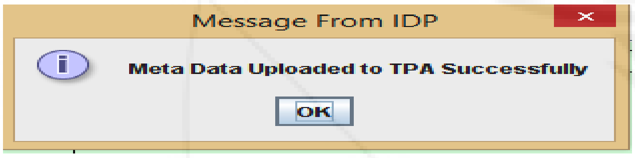
Figure 6.4: Sending Metadata to TPA



Enter the TPA IPAddress

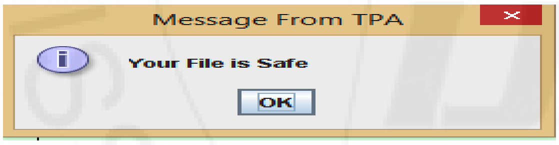
127.0.0.1

Figure 6.5: Entering TPA's IP address



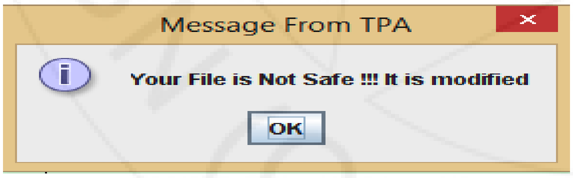
Meta Data Uploaded to TPA Successfully

Figure 6.6: Message after uploading metadata



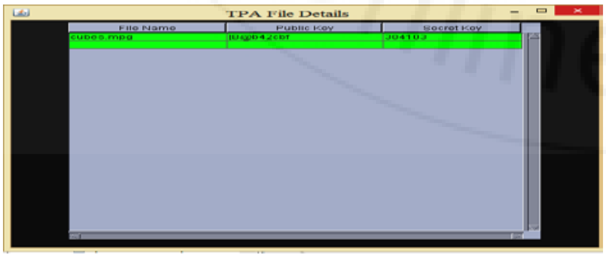
Your File is Safe

Figure 6.7: Message from TPA



Your File is Not Safe !!! It is modified

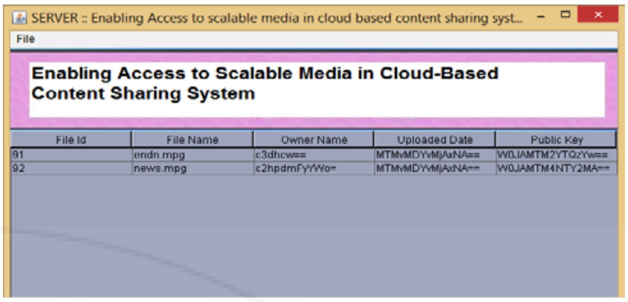
Figure 6.8: Message to indicate file has been modified



File Name	Public Key	Secret Key
cubes.mpg	jUgb42cbf	J04103

Figure 6.9: TPA File Details

As shown in above fig 6.9, TPA maintains some details about file which contains filename, public key and secret key of that particular file. If any user wants to access the file then, user should request to TPA. TPA maintains secret key for every file, if authorized user request for key then TPA will send secret key for that file.

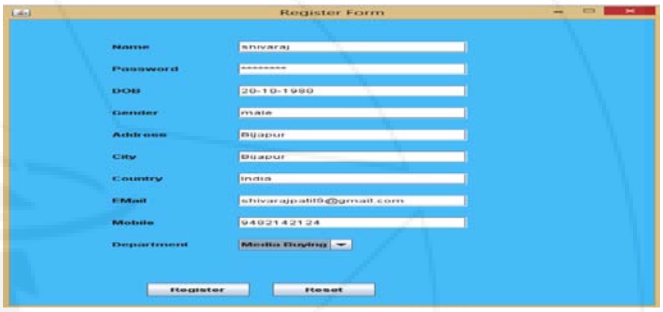

SERVER :: Enabling Access to scalable media in cloud based content sharing syst...
File

Enabling Access to Scalable Media in Cloud-Based Content Sharing System

File Id	File Name	Owner Name	Uploaded Date	Public Key
91	endn.mpg	c3dhcw==	MTMvMDYvMjAxNA==	W0JAMTM2YTQzYw==
92	news.mpg	c2hpdmFyYWo=	MTMvMDYvMjAxNA==	W0JAMTM4NTY2MA==

Figure 6.10: CSP Page

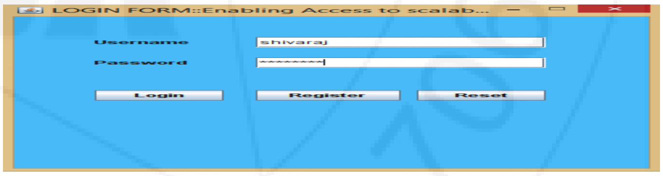
As shown in above fig 6.10 CSP provides the storage space for the files, in which authorized users upload the files. In CSP the attributes of files like owner name, uploaded date and public key all are in encrypted form. It's because there is a possibility that sometimes, third party compromise with data owners for accessing the data.



Name	shivaraj
Password	********
DOB	20-10-1980
Gender	male
Address	Bijapur
City	Bijapur
Country	india
EMail	shivarajpatil9@gmail.com
Mobile	9482142124
Department	Media Buying

Figure 6.11: User registration form

As shown in above fig 6.11 shows the registration form for users, in which users will register by providing attributes. In this, users will register in department wise in which, they will access the files according to their privileges.

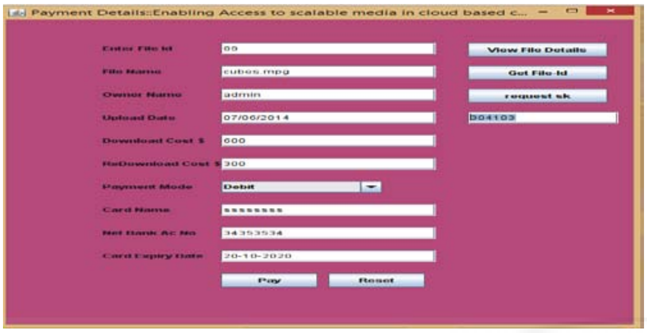


Username	shivaraj
Password	*********

Figure 6.12: User login page

Figures 6.12-6.14 show the steps for accessing the data from cloud. In this first user will login into cloud for accessing the data. After login user will access files which lies in respective user's access level. After selecting the particular file, user will request for a secret key for that file to TPA. TPA maintains secret key for every files in which, after getting request, TPA will send the key to user. After getting the key user will get access to that file by payment methods.

Licensed Under Creative Commons Attribution CC BY

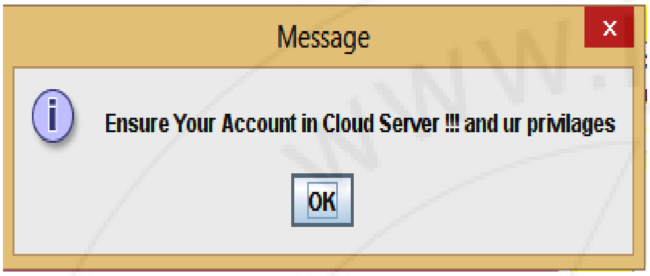


Payment Details::Enabling Access to scalable media in cloud based c...

Enter File Id	00
File Name	cubes.mpg
Owner Name	admin
Upload Date	07/06/2014
Download Cost $	600
ReDownload Cost $	300
Payment Mode	Debit
Card Name	ssssssss
Net Bank Ac No	34353534
Card Expiry Date	20-10-2020

b04103

Figure 6.13: User requesting For SK and Payment Details



Message

Ensure Your Account in Cloud Server !!! and ur privilages

Figure 6.14: Message from TPA for denied-privileged access

7. Conclusion and Future Work

In this project, we have developed a system that solves the problem of data integrity, unauthorized access, privacy, consistency and also it aims for maintaining fine-grained data access control in cloud computing. This scheme presents a network in which cloud architecture, users, and TPA are shown, after that it describes retrieval of file, encryption and decryption of file, how to check the integrity of data from CSP and how to give control to TPA. Further, challenging issues for public auditing services that need to be focused. It is believed that security in cloud computing is very much needed as data in cloud storage are not secure. This project can be extended to incorporate efficient user revocation scheme.

References

[1] Josh Ames, http://blog.appcore.com/.

[2] http://www.cloud-competence-center.com/

[3] Neuman, C., and Ts'o, T. Kerberos: An authentication service for computer networks. IEEE Computer 32, 9 (September 1994).

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peter-son, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08. New York, NY, USA: ACM, 2008, pp. 1–10.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, Charleston, South Carolina, USA, 2009.

[7] Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.

[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of ASIACRYPT'08. Melbourne, Australia: Springer-Verlag, 2008, pp. 90–107.

[9] Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Cryptology ePrint Archive, Report 2008/432, 2008.

[10] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[11] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[12] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.

[13] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT '04), Lecture Notes in Computer Science. Springer Verlag, 2004.

[14] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.

[15] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.

[16] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http: //seclab.cs.ucdavis.edu/projects/history/.

[17] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March 2010.

[18] Kuyoro S. O., Ibikunle F. & Awodele O, Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[19] http://cloudtweaks.com/.

[20] Barrie Sosinsky, Cloud Computing Bible, Wiley India Pvt Ltd,2011.

[21] Greg Boss, Cloud Computing IBM 2007.10

[22] http://cloudtweaks.com/.

[23] Greg Boss, Cloud Computing IBM 2007.10

Licensed Under Creative Commons Attribution CC BY