ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Enabling Mutual Trust for Cloud Storage Systems Using Cheating detection module

Noorandayya R Swamy[1], Dr. D. R Shashi Kumar[2]

Student- M.Tech, Department of CS&E Cambridge Institute of Technology, Bangalore, India [1]

HOD, Department of CS&E, Cambridge Institute of Technology, Bangalore, India[2]

Abstract: Currently, the amount of sensitive data produced by many organizations is out pacing their storage ability. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, a cloud-based storage scheme is proposed that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has two important features: i) It allows the owner to outsource sensitive data to a CSP, and it ensures that only authorized users (i.e., Those who have the right to access the owner's file) receive the outsourced data i.e. It enforces the access control of the outsourced data can be done by sending a key through email to the registered users and ii) Enables indirect mutual trust between the owner and the CSP using Cheating detection module.

Keywords: Outsourcing data storage, dynamic environment, mutual trust, CSP, Cheating detection module, access control, TTP.

I. INTRODUCTION

Cloud computing is playing an important role in current era, because of its flexibility, Massive Web-scale abstracted infrastructures, Dynamic allocations, Scaling, Movement of Applications, No long-term commitments and No hardware or software to install. So this results in Business and IT-aligned benefits are: Provides an effective and creative service delivery module, Delivery services in a less costly and higher quality business model while providing service access ubiquity, Rapidly deploy applications over the internet and leverage new technologies to deliver services When, Where and How your Clients needs them.

The Data produced in the Organization is Huge and very Confidential and maintaining this data to the organization is challenging so they may go for outsourcing the data to CSP, This data may be Distributed and stored for a long time due to operational purposes and regulatory compliance. The local management of such huge amount of data is problematic and costly. While there is an observable drop in the cost of storage hardware, the management of storage has become more complex and represents approximately 75% of the total ownership cost.

Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. The proposed model provides trusted computing environment by addressing important issues related to outsourcing the storage of data, namely confidentiality, integrity, access control and mutual trust between the data owner and the CSP. This means that the remotely stored data should be accessed only by authorized users (i.e., those who have the right to access the owner's file) and should remain confidential. The CSP needs to be safeguarded from any false accusation that may be claimed by a data owner to get illegal compensations.

In this work, we propose a scheme that addresses some important issues related to outsourcing the storage of data, namely data dynamic, newness, mutual trust, and access control. One of the core design principles of data outsourcing is to provide dynamic scalability of data.

1.1 The main contributions of this paper are:

1) The design and implementation of a cloud-based storage scheme has. It allows a data owner to outsource the data to a remote CSP, and perform full dynamic operations at the block-level, i.e. it supports operations such as block modification, insertion ,deletion, and append It ensures the newness property, i.e., the authorized users receive the most recent version of the data.

2) Detection of False accusation by using Cheating detection module.

2. EXISTING SYSTEM

A solution to detect cheating from owner side as well as CSP side is done through digital signatures. For each file owner attaches digital signature before outsourcing. The CSP first verifies digital signature of owner before storing data on cloud. In case of failed verification, the CSP rejects to store data and asks the owner to resend the correct signature. If the signature is valid, both the file and signature are stored on the cloud servers. The digital signature achieves non-repudiation from the owner side. When an authorized user (or the owner) requests to retrieve the data file, the CSP sends file, owner's signature and CSP's signature on (file || owner's signature). The authorized user first verifies the CSP's signature. In case of failed verification, the user asks CSP to re-perform the transmission process. If CSP's signature is valid, the user then verifies owner's signature. If verification fails, this indicates the corruption of data over the cloud servers. The CSP cannot repudiate such corruption for the owner's signature is previously verified and stored by the CSP along with file. Since CSP's signature is attached with the received data, a dishonest owner cannot falsely accuse the CSP regarding data integrity.

The above solution increases the storage overhead on cloud as owner's signature is stored along with the file on cloud servers. Moreover, there is an increased computation overhead, CSP has to verify signature of owner before storing file on cloud, and the authorized user verifies two signatures for each received file. If the CSP receives file from trusted entity other than the owner, the signature verification is not needed since the trusted entity has no incentive for repudiation or collusion. Therefore, delegating small part of owner's work to the TTP reduces both the storage and computation overheads. However the outsourced data must be kept private and any leakage of data toward the TTP must be prevented

Limitations

1. The CSP is untrusted, and thus the confidentiality and integrity of data in the cloud may be at risk.
2. Computation Overhead is more in owner side As well as CSP side
3. A data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement.
4. The Owner May Loss the direct control over the sensitive data.

3.PROPOSED SYSTEM

3.1 System Model

3.1.1 Owner Model.

That can be an organization / individual generating sensitive data to be stored in the cloud and made available for controlled external use.

3.1.2 Cloud service provider (CSP)

Who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users.

3.1.3 Authorized Users

A set of owner's clients who have the right to access the remote data.

3.1.4 Trusted Third Party (TTP)

An entity who is trusted by all other system components, and has capabilities to detect/specify dishonest parties.

The cloud computing storage model considered in this work consists of four main components as illustrated in Figure 1. The relations between different system components are represented by double-sided arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the data owner, the authorized users, and the CSP trust the TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to enable indirect mutual trust between these three components. There is a direct trust relationship between the data owner and the authorized users.

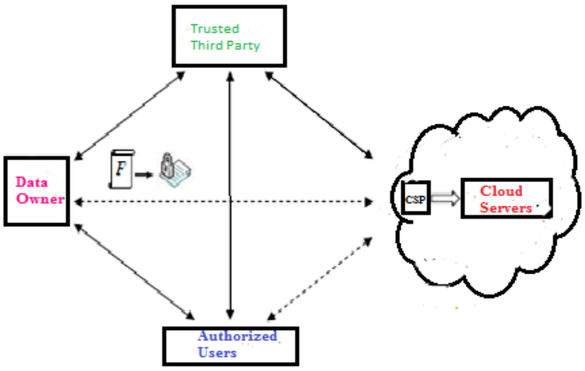


Fig 1: Cloud computing data storage system model

3.2 Updating and Access Control

The Outsourcing of the confidential data has been done by the data owner to the cloud storage servers in an encrypted form. When the authorized users request for data, they will get data in an encrypted form this data can be decrypted by them using the secret key shared among the authorized users. It is assumed that the interaction between the owner and the authorized users to authenticate their identities has already been completed, and it is not considered in this work.

The TTP and CSP must be always Online, while the owner is intermittently Online .The authorized users able to access data file from CSP even when the owner is offline.

3.3 Cheating model

The CSP resides in an untrusted domain and thus the confidentiality and integrity of data in the cloud may be at risk. For economic incentives and maintaining a reputation, the CSP may hide data loss, or reclaim storage by discarding data that have not been or is rarely accessed. On the other hand, a data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement. They may dishonestly claim that data integrity over cloud servers has been violated.

3.4 Security Requirements

3.4.1 Confidentiality

Outsourced data must be protected from the TTP, the CSP, and users that are not granted access.

3.4.2 Integrity

Outsourced data are required to remain intact on cloud servers. The data owner and authorized users must be enabled to recognize data corruption over the CSP side.

3.4.3 Access control

Only authorized users are allowed to access the outsourced data.

3.4.4 CSP's Defence

The CSP must be safeguarded against false accusations that may be claimed by dishonest owner/users, and such a malicious behaviour is required to be revealed.

4. FRAMEWORK

Framework consists of notations, setup and file preparation for data outsourcing, data, access and cheating detection of dishonest owner/user.

4.1 Notations

- F is a data file to be outsourced
- h is a cryptographic hash function
- k is a data encryption key/secret key
- Ek is a symmetric encryption algorithm under, e.g., AES (advanced encryption standard) K
- E-1K is a symmetric decryption algorithm under K
- F1 is an encrypted version of the file F
- F1HTTP is a hash value for F1 , and is computed and stored by the TTP
- F1Hu is a hash value for F1 , and is computed by the authorized user
- ENCs(K) is an encrypted version of secret key under S
- is a secret shared between owner and his authorized users. S

4.2 file preparation for data outsourcing

The system setup has two parts: one is done on the Owner side, and the other is done on the TTP side and CSP will stores only encrypted file as shown in figure 2.

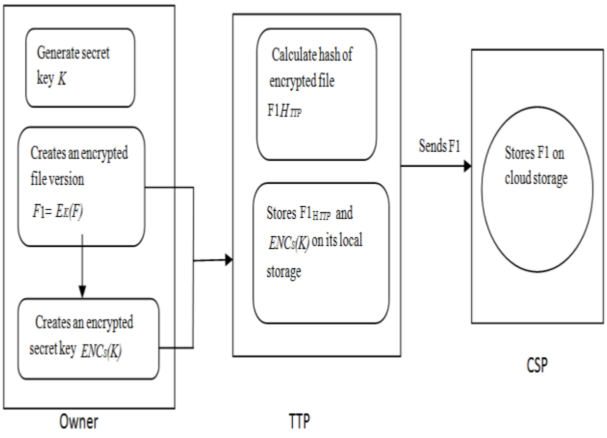

Generate secret key K
Creates an encrypted file version
$F1= E_K(F)$
Creates an encrypted secret key $ENC_S(K)$
Owner
Calculate hash of encrypted file
$F1H_{TTP}$
Stores $F1H_{TTP}$ and $ENC_S(K)$ on its local storage
TTP
Sends F1
Stores F1 on cloud storage
CSP

Fig 2: file preparation for data outsourcing

4.2.1 Owner role

The data owner generates a secret key K for a file. To achieve privacy-preserving, the owner creates an encrypted file version F1=Ek(F) . For access control he creates encrypted secret key enables only authorized users to decrypt secret key and access the outsourced file. The owner sends F1 and ENCs(K) to the TTP, and deletes the data file from its local storage.

4.2.2 TTP role

A small part of the owner's work is delegated to the TTP to reduce the storage overhead and lower the overall system computation. For the TTP to resolve disputes that may arise regarding data integrity it computes and locally stores hash value for the encrypted file F1HTTP . The TTP sends encrypted file F1 to the CSP. The TTP keeps only F1HTTP and ENCs(K) on its local storage.

4. 3 Data Access and Cheating Detection

An authorized user sends a data-access request to both the CSP and the TTP. The authorized user receives F1 from the CSP and (F1HTTP, ENCs (K)) from the TTP.

4.3.1 Verification of encrypted data file

The authorized user computes hash of encrypted file F1Hu received from the CSP and compare it with one received from the TTP F1HTTP . If F1HTTP ≠ F1Hu then invoke cheating detection procedure at TTP. And if F1HTTP = F1Hu then decrypts ENCs(K) to get Secret Key K and hence decrypts file. Data Access and Verification of encrypted data file is shown in figure 3.

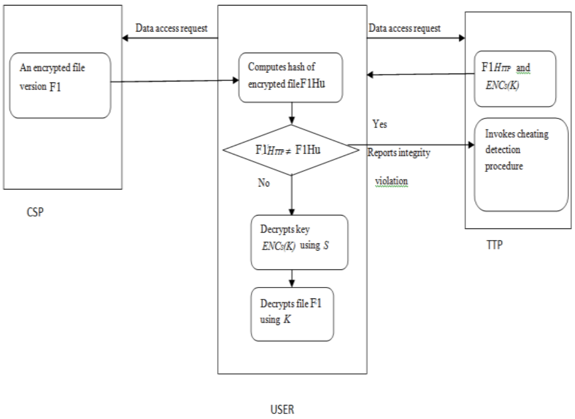

Data access request
Data access request
An encrypted file version F1
CSP
Computes hash of encrypted fileF1Hu
$F1H_{TTP} \neq F1Hu$
Yes
No
Reports integrity violation
Decrypts key $ENC_S(K)$ using S
Decrypts file F1 using K
USER
$F1H_{TTP}$ and $ENC_S(K)$
Invokes cheating detection procedure
TTP

Fig 3: Data Access and Verification of encrypted data file

4.3.2 Cheating detection procedure

TTP is invoked to determine the dishonest party. The TTP receives encrypted file F1 from the CSP and computes temporary hash value for encrypted file F1Htemp. If F1HTTP ≠ F1Htemp then reports "dishonest CSP and data is corrupted" to owner. If F1HTTP = F1Htemp then reports "dishonest owner/user and data is not corrupted". Cheating detection procedure is shown in figure 4.

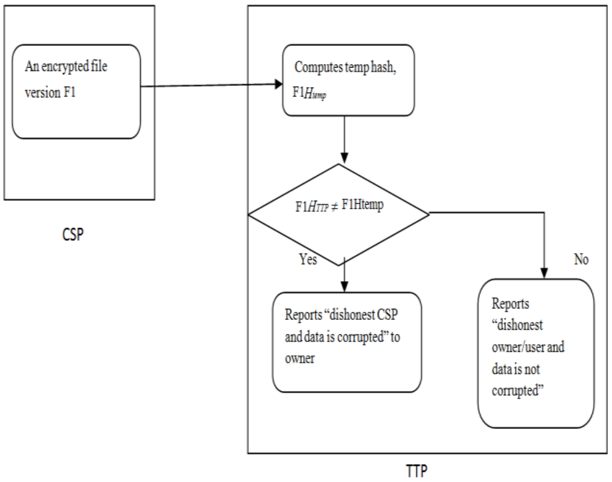

An encrypted file version F1
CSP
Computes temp hash, F1Htemp
F1H_TTP ≠ F1Htemp
Yes
No
Reports "dishonest CSP and data is corrupted" to owner
Reports "dishonest owner/user and data is not corrupted"
TTP

Fig 4: Cheating detection procedure

1. SECURITY RELATED ANALYSIS

1.1 Detection of dishonest owner/user

If the owner/user falsely accuses the CSP regarding data integrity, the TTP performs cheating detection procedure. In this procedure, TTP retrieves encrypted file from CSP and computes the temporary hash value F1Htemp and compares F1HTTP and F1Htemp. If F1HTT =F1Htemp then F1 has not been corrupted on the server and owner/ user is dishonest.

5.2 Detection of dishonest CSP

During the data access phase of the proposed scheme, the authorized user receives the encrypted file F1 from the CSP and F1HTTP from the TTP. The authorized user computes hash of encrypted file F1Hu and compares F1HTTP and F1Hu.

If F1HTP /= F1Hu, a report is issued to TTP to determine the dishonest party. The TTP retrieves encrypted file from CSP and computes the temporary hash value F1Htemp and compares F1HTTP and F1Hu .If F1HTTP ≠F1Htemp, then F1 has been corrupted on the server and CSP is dishonest.

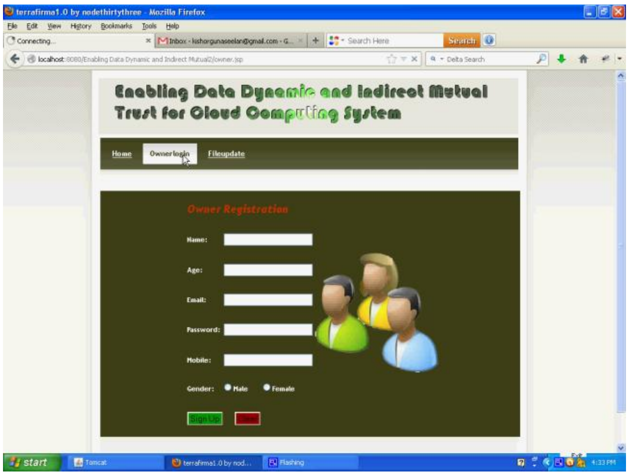
1. IMPLEMENTATION

The proposed scheme is implemented using HTML, JSP and Java i.e Web Application. The proposed scheme consists of six modules: User Registration, Owner Registration, User Login, Owner Login, TTP Module, TTP Alert Module and CSP Module. The User Registration Module will take the required information from the User i.e. Name, email-id, Password, Employee code and Mobile Number and Stores in Database. The Owner Registration Module will take the required information from the Owner i.e. Name, email-id, Password, Employee code and Mobile Number and Stores in Database. The User Login Module Accepts the Email-id and Password from the User and Validate These Credentials with the Database if These Information is correct Then it will allow them to Login. The Owner Login Module Accepts the Email-id and Password from the Owner and Validate These Credentials with the Database if These Information is correct Then it will allow them to Login. The TTP Module also had a TTP Login it will ask them to enter Valid User Name and Password, After Login the TTP module will have the Files which are uploaded by the Owner. The TTP Alert Module Will check for the Dishonest Party (i.e. Owner or CSP) by comparing File which is stored in its database as well as File sent from the Authorized User if they want. The CSP Module also had a CSP Login it will ask them to enter Valid User Name and Password, After Login the CSP module will have the Files which are uploaded by the TTP

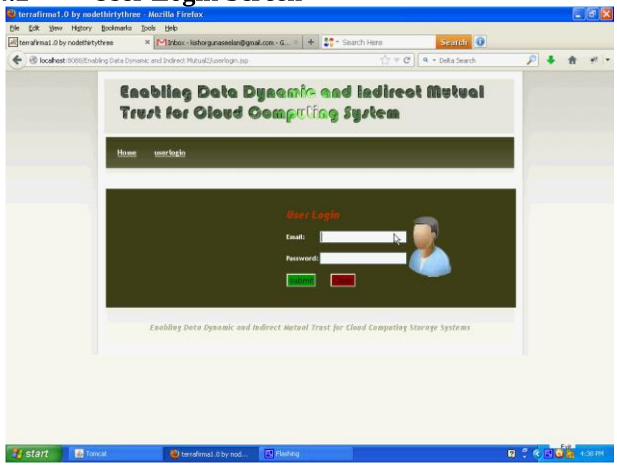
1.1 Implementation settings

In implementation, a laptop HCL with Intel® Core™ (2.20 GHz, 2 MB L2 cache) processor and 2 GB RAM running Microsoft Windows 7 OS.
Using Eclipse we have developed a Dynamic Web Application and installed Using apache-tomcat-7.0.25 and Finally an Email Service.

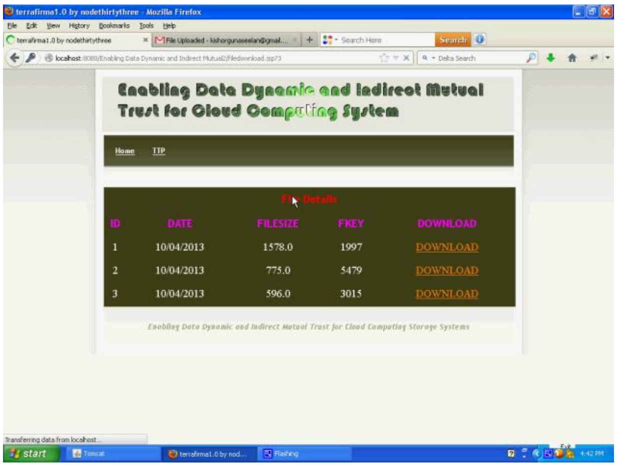
4.1 Owner Registration Screen


terrafirma1.0 by nodethirtythree - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
Inbox - kishorgunaseelan@gmail.com - G...
Search Here
Search
localhost:8080/Enabling Data Dynamic and Indirect Mutual2/owner.jsp
Delta Search
Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing System
Home
Ownerlogin
Fileupdate
Owner Registration
Name:
Age:
Email:
Password:
Mobile:
Gender: ○ Male ○ Female
Sign Up
Clear
start
Tomcat
terrafirma1.0 by nod...
Flashing
4:33 PM

4.2 User Login Screen


terrafirma1.0 by nodethirtythree - Mozilla Firefox
File Edit View History Bookmarks Tools Help
terrafirma1.0 by nodethirtythree
Inbox - kishorgunaseelan@gmail.com - G...
Search Here
Search
localhost:8080/Enabling Data Dynamic and Indirect Mutual2/userlogin.jsp
Delta Search
Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing System
Home
userlogin
User Login
Email:
Password:
submit
clear
Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems
start
Tomcat
terrafirma1.0 by nod...
Flashing
4:38 PM

4.3 TTP Module Screen



Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing System

Home TTP

File Details

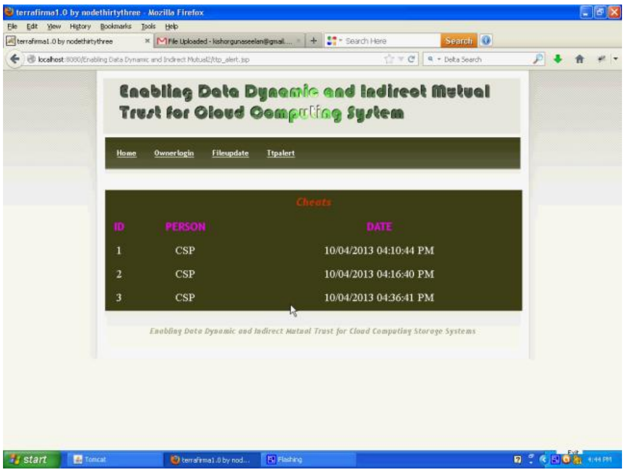
ID	DATE	FILESIZE	FKEY	DOWNLOAD
1	10/04/2013	1578.0	1997	DOWNLOAD
2	10/04/2013	775.0	5479	DOWNLOAD
3	10/04/2013	596.0	3015	DOWNLOAD

Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems

Transferring data from localhost...

terrafirma1.0 by nodethirtythree - Mozilla Firefox
localhost:8080/Enabling Data Dynamic and Indirect Mutual2/filedownload.jsp?3

1.1 TTP Alert Module Screen



Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing System

Home Ownerlogin Fileupdate Ttpalert

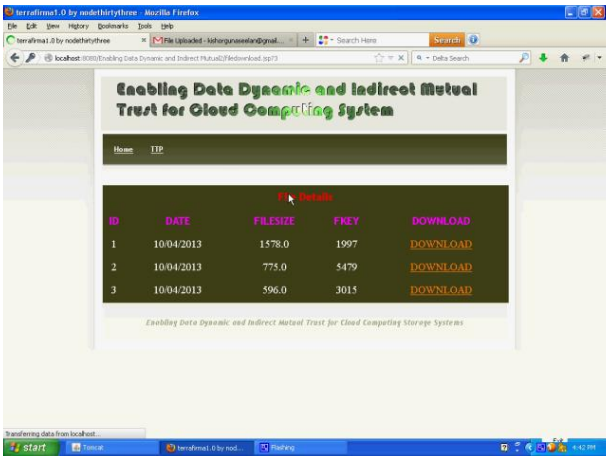
Cheats

ID	PERSON	DATE
1	CSP	10/04/2013 04:10:44 PM
2	CSP	10/04/2013 04:16:40 PM
3	CSP	10/04/2013 04:36:41 PM

Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems

terrafirma1.0 by nodethirtythree - Mozilla Firefox
localhost:8080/Enabling Data Dynamic and Indirect Mutual2/ttp_alert.jsp

1.2 CSP Module Screen



Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing System

Home TTP

File Details

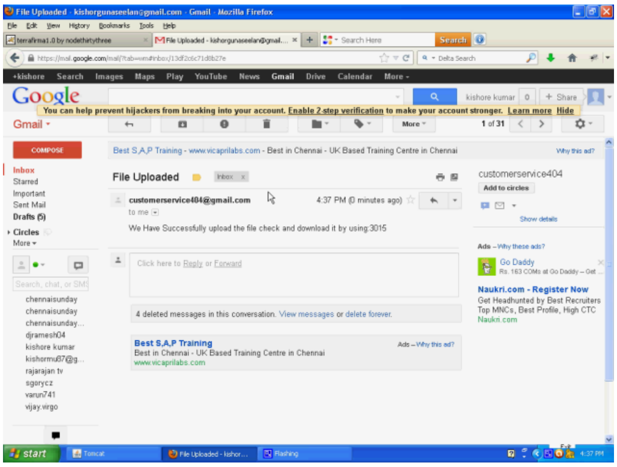
ID	DATE	FILESIZE	FKEY	DOWNLOAD
1	10/04/2013	1578.0	1997	DOWNLOAD
2	10/04/2013	775.0	5479	DOWNLOAD
3	10/04/2013	596.0	3015	DOWNLOAD

Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems

Transferring data from localhost...

terrafirma1.0 by nodethirtythree - Mozilla Firefox
localhost:8080/Enabling Data Dynamic and Indirect Mutual2/filedownload.jsp?3

1.3 Key Sent to the User Email, Screen



File Uploaded

customerservice404@gmail.com 4:37 PM (0 minutes ago)
to me

We Have Successfully upload the file check and download it by using:3015

Click here to Reply or Forward

4 deleted messages in this conversation. View messages or delete forever.

File Uploaded - kishorgunaseelan@gmail.com - Gmail - Mozilla Firefox
https://mail.google.com/mail/?tab=wm#inbox/13df2c6c71d8b27e
You can help prevent hijackers from breaking into your account. Enable 2-step verification to make your account stronger. Learn more Hide
Gmail
COMPOSE
Inbox
Starred
Important
Sent Mail
Drafts (5)
Circles
More
1 of 31
customerservice404
Add to circles
Show details

1.1 File Upload

First the Owner uploads their data (i.e. File) while uploading the data is encrypted and Key has been generated for a particular file, and it should be unique to a file, The encryption algorithm implemented here is Advanced Encryption Standard (AES), Then this file is by Default sent to the TTP as well as CSP, with corresponding Key.

In the TTP, It will verify the data and Key, Stores it into database.

When the Authorized Users Request For a particular File they have to Login with the valid username and password which is registered, to retrieve the file from the CSP they need a key Which is given by the owner to an authorized user using that key they can decrypt the file and that key is sent to the registered E-mail .

1.2 Cheating Detection

The Cheating Detection is enabled by the TTP alert Module

If users or customers raised an issue regarding the data security the TTP alert Module will compares the Particular file with the other file which is stored in its own database, If file is same as the file which is stored in the TTP database then there will be the Dishonest Owner and If the file is not same as the file which is stored in the TTP database then there will be Dishonest CSP, Likewise it will detect the Dishonest Party either Owner or CSP.

CONCLUSION

The cloud based storage scheme is proposed that allows owner to benefit from facilities offered by the CSP and enables Detection of Dishonest entity (i.e. owner/CSP).

It enables data owners to release their concerns regarding confidentiality, integrity, access control of the outsourced data. To resolve disputes that may occur regarding data integrity, a trusted third party is invoked to determine the dishonest party (owner or CSP). Also the security related issues are resolved they are: (i) Access control is enabled using the Login Modules of each entity, while Login It will validate the credentials given by the each entity. (ii) Data Confidentiality is achieved using the encryption algorithms. (iii) Detection of Dishonest Owner/CSP Using the TTP alert module.

1. FUTURE RESEARCH DIRECTIONS

The area of cloud computing has attracted many researchers from diverse fields; however, much effort remains to achieve the wide acceptance and usage of cloud computing technology. A number of future research directions stem from our current research. Below, we summarize some problems to address during our future research

1.1 Storage Overhead in TTP

The files which are Outsourced to the CSP from the data owner all these files has to stored in the TTP, This is necessary in detection of Dishonest party, But the storage space required to store the data is huge and it will take sustainable cost as well and also the maintenance of that particular data, The research may be proceeded to minimize the data stored in the TTP.

REFERENCES

[1] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws.amazon.com, 2008.

[2] K. E. Fu, “Group sharing and random access in cryptographic storage file systems,” Master’s thesis, MIT, Tech. Rep., 1999.

[3] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, “Enabling security in cloud storage SLAs with cloud proof,” in Proceedings of the 2011 USENIX conference, 2011.

[4] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficient access to outsourced data,” in Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 55–66.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,“Plutus: Scalable secure file sharing on untrusted storage,” in Proceedings of the FAST 03: File and Storage Technologies, 2003.

[6] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short cipher texts and private keys,” in Advances in Cryptology - CRYPTO, 2005, pp. 258–275.

[7] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, “Efficient remote data possession checking in critical information infrastructures,” IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.

[8] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, 2008, pp. 1–10.

BIOGRAPHY

Noorandayya. R. Swamy is an M.Tech student of Cambridge Institute of Technology, Bangalore, India Presently he is pursuing his M.Tech [CSE] from this college Doing His Academic project Under the Guidance of Dr. D. R Shashi Kumar HOD Department of CS&E and he received his B.E from Rural Engineering College Bhalki, affiliated to VTU University, in the year 2011. His area of interest includes Cloud computing and Object oriented Programming languages, all current trends and techniques in Computer Science.