Secure data transmission in cloud computing with trusted third party using encryption/decryption technique

S.Kavipriya
Kavichitra08@gmail.com
Department of CSE
IFET college of engineering
D.Jaya Kumar
Jayakumar1988@hotmail.com
Senior assistant professor
Department of CSE
IFET college of engineering

Abstract:
Off-site data storage is a one of the application into the cloud that relieves the customers from focusing on data storage system. However the outsourcing data to a third-party organizational control entail serious security concerns. Data leakage may occur due to attack by other users and machines in the cloud. Since it involves multiple steps in encryption and decryption it will takes more time. To proposed some of the data security for cloud environment for trusted third party and then data security will be provides (a) key management (b) access control, and (c) file assured deletion. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. We use multiple key managers, each hosting one share of key. Multiple key managers avoid single point of malfunction for the cryptographic keys.

INTRODUCTION

Cloud Computing is packaged within a new transportation paradigm that offers improved scalability, flexibility, startup time, condensed costs, and just-in-time availability of resources. Cloud computing has emerge as supervision the hardware and software assets located at third-party competence provider. Demand way in to the computing property relieve the customers from building and maintaining complex infrastructures .Cloud computing has every computing component as a value , such as software, platform, and infrastructure. Multiple users, separated through virtual machines, share resources as well as storage space. Multi-tenancy and virtualization generate risks and underpins the confidence of users to adopt the cloud model. The security of outsourcing data to public clouds, work for the development of data security technique. They have three entities are data owner, user and the cloud server. The FADE is lightweight scalable methods that give surety the deletion of files from cloud when requested by the user .During our inspection FADE short on issues of security of keys and authentication of participating parties. Based on that identified with FADE, development to the scheme and name it as Data Security for Cloud Environment with Trusted Third Party for group data sharing and forwarding .the man-in-the-middle-attack, we steps for the session key establishment process. The security level and exclude the wicked user to carry out the attack at a performance. The grades from our confirmation investigation Successful authentication and session key concern amount produced in contact to symmetric keys are mainly use in consequent cryptographic operations. The integrity of data for symmetric key and Message Authentication Code and securing symmetric keys to generated by third party key managers.

LITERATURE SURVEY

[1]Data Security for Cloud Environment with Semi-Trusted Third Party

We propose Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a data security system that provides key management access

control, and file assured deletion.We use multiple key managers, each hosting one share of key. Multiple key managers avoid single point of breakdown for the cryptographic keys.Access to key and data is ensured through a policy file that states policies under which access is arranged to the keys. The client generates random symmetric keys for performing encryption and integrity functions.Symmetric keys are protected by the public key, which are generated by the key managers.

[2]Enhancement for data security in cloud computing environment

It aims to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entity, and using the advanced business model like SaaS (Software as a Service) to distribute the powerful computing capacity to end users hands. To address this long standing limitation by building a multi-tenant system. Our system provides the environment for the user to perform his tasks, but with very high security. By using further facilities provided in this system user fill secure about his data and his account.

[3]A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding

Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. . We propose a threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back.

[4]Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment

we propose a new cloud computing environment where we approach a trusted cloud environment which is controlled by both the client and the cloud environment admin.. This provides a way to hide the data and normal user and can protect their data from the cloud provider. This provides a two way security protocol which helps both the cloud and the normal user. When the cloud user upload the data in the cloud environment, the data is uploaded in encrypted form using RSA algorithm and the cloud admin can decrypt using their own private key.

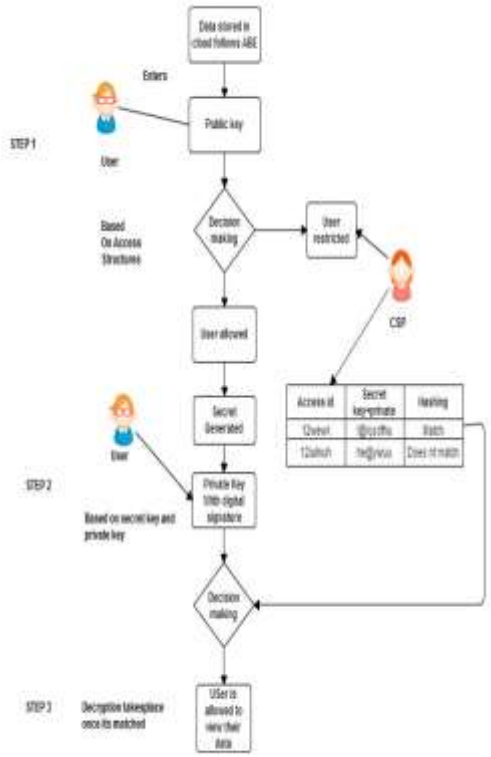
SYSTEM ANALYSIS

EXISTING SYSTEM

A cloud storage security system that provided key management, access control, and file assured deletion. Assured deletion was based on policies associated with the data file uploaded to cloud.On revocation of policies, access keys are deleted by the key management that result in halting of the access to the data. Therefore, the files were logically deleted from the cloud. The results revealed that the DaSCE protocol can be practically used for clouds for security of outsourced data. The fact that the DaSCE does not require any protocol and implementation level changes at the cloud makes it highly practical methodology for cloud. In future, the DaSCE methodology can be extended to secure group shared data and secure data forwarding. Since it involves multiple steps in encryption and decryption it will takes more time. Once the user forgets user id and password they can't decrypt the file (Once the authentication fails it doesn't move to next step).

PROPOSED SYSTEM

Cloud computing is anpromising, on-demand and internet- based technology. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. This technology has been used by worldwide customers to improve their business performance. This paper presents the strict authentication system by introducing the multi-level authentication technique which generates/authenticates the password in multiple levels to access the cloud services. Once they forget the username and password then they can easy to retrieve the data easily by using pass key
A password isa word or string of characters used for user authentication to prove identity or access approval to gain access to a resource which should be kept secret from those not allowed access. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobilephones, cable
TV decoders, automated teller machines (ATMs), etc.



MODULES

[1]New user registration :

In this module user to register to become a cloud member, and then once they will be registered in some kind of attributes like(name,email,phone,address) and then some of the user will be encrypted the file from the policy that has been created.

[2]Encrypted data creation:

It has collection of document like S={s1,s2,s3,…….,sn}that has to be encrypted the data to the cloud server.we use an algorithm for the encrypt the data into the cloud server is AES algorithm.Here the RSA is expensive than the AES algorithm.

[3]Decrypted the data:

If the user need to download the file, they will send the request to the key manager with the appropriate attributes.the key manager will be checking the attributes and decrypt to the appropriate user.now the user will be receive the secret key and then downloaded the file and their decrypt with the secret key.

CONCLUSION

We proposed the DaSCE protocol by using ABE algorithm, a cloud storage security system that provided key management, access control, and file assured deletion. Assured deletion was based on policies associated with the data file uploaded to cloud. On revocation of policies, access keys are deleted by the *KMs* that result in halting of the access to the data. There-fore, the files were logically deleted from the cloud. The key management was accomplished using (*k, n*) threshold secret sharing mechanism.

REFERENCE

[1] M. ARMBRUST, A. FOX, R. GRIFFITH, A.D. JOSEPH, R. KTAZ, A. KONWIN-SKI, G. LEE, D. PATTERSON, A. RABKIN, I. STOICS, AND M. ZAHARIA, "A VIEW OF CLOUD COMPUTING," *COMMUNICATIONS OF THE ACM*, VOL. 53, NO. 4, 2010, PP. 50-58.

[2] M. S. BLUMENTHAL, "IS SECURITY LOST IN THE CLOUDS?"*COMMUNICA-TIONS AND STRATEGIES*, NO. 81, 2011, PP. 69-86.

[3] C.CACHINANDM.SCHUNTER, "A CLOUD YOU CAN TRUST,"*IEEESPECTRUM*,VOL. 48, NO. 12,2011,PP. 28-51.

[4] C. CREMERS, "THE SCYTHER TOOL: VERIFICATION, FALSIFICATION, AND ANALYSIS OF SECURITY PROTOCOLS." *IN COMPUTER AIDED VERIFICATION, SPRINGER BERLIN HEIDELBERG*, 2008, PP. 414-418.

[5]CLOUD SECURITY ALLIANCE HTTPS://DOWNLOADS.CLOUDSECURITYALLIANCE.ORG/INITIATIVES/CDG/CSA_CCAQIS_SURVEY.PDF (ACCESSED MARCH 24, 2013).

[6] W. DIFFIE, P. C. V. OORSCHOT, AND M. J. WIENER, "AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES,"*DESIGNS, CODES AND CRYPTOGRAPHY*,VOL. 2, NO. 2, 1992, PP. 107-125.

[7]M. Ali, K. Bilal, S. U. Khan, B. Veeravalli, K. Li, and A. Y. Zomaya, "DROPS: Division and Replication of Data in the Cloud for Opti-mal Performance and Security," *IEEE Transactions on Cloud Computing*, 2015, DOI: 10.1109/TCC.2015.2400460.

[8] N. En and N. Srensson, "An extensible SAT-solver," *Lecture Notes in Computer Science*, vol. 2919, Springer, 2003, pp. 502-518.

