ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Novel Approach for Secure Group Data Sharing and Forwarding in Cloud Environment

N.Vishnudevi[1], P.E.Prem[2], M.Madlinasha[3]

[1]PG Student [IT], Dept. of IT, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India

[2]Assistant professor, Dept. of IT, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India

[3]Assistant professor, Dept. of IT, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India

ABSTRACT*:* Off-Site data storage is a function of cloud that relieve the customers from focus on data storage cloud computing organization. Out sourcing data to third-party administrative control makes security problem. Data leakage may occr due to attacks by other users in the cloud. Comprehensive of data by cloud service provider is yet another problem in the cloud because of that high level of security is needed . In this paper provide high security by the concept of Data Security for Cloud Environment with Semi-Trusted Third Party for secure group data sharing and forwarding. It provides for key management**,** access control, and file assured deletion. The DaSCE use Shamir entry system to handle and generate the key. We use multiple key managers for one share of key. many key managers avoid on its own failure by using cryptographic keys.We execute and estimate running model of DaSCE performance based on the time consumption when more number operations, next analyze the working of DaSCE using High Level Petri nets .The outcome can be efficiently used for security measures of outsourcing data by key management, access control, and file assured deletion.

KEYWORDS*:* Cloud Computing , High Level Petri Nets,file assured deletion,key management,shamir scheme

I.INTRODUCTION

Cloud Computing is packaged within a new infrastructure paradigm that offers improved scalability, elasticity, startup time, reduced costs, and just-in-time availability of resources.Cloud computing has emerge as managing the hardware and software assets located at third-party facility provider.Demand way in to the computing resources relieve the customers from building and maintaining complex infrastructures.Cloud computing has every computing component as a utility ,such as software, platform, and infrastructure. The cost-cutting measure of infrastructure, maintenance, and flexibility makes cloud computing smart for organizations and individual customers.although benefits, cloud computing faces assured challenges and issues widespread adoption of cloud.For instance,security, performance, and quality are mentioned. security , privacy unease when using cloud computing services are like to those of traditional non-cloud services, apprehension are amplified by external control over executive resources and the potential for mismanagement of those resources. Transitioning to public cloud computing involve a transfer of responsibility and control to the cloud provider over information system Representing characteristics and c utility ,causes the user to focus on data security, transmission, processing , moving data to the cloud, and operated by certain level of trust and security. 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. We aim for a technique capable of addressing the critical issues. data security scheme that uses key manager servers for the cryptographic keys. Shamir's (k, n) threshold scheme is used for the management of keys that use k share out of n in the direction of reconstruct the key. Access to key and data is ensured through a policy file.The client generates random symmetric keys for encryption and integrity functions. Symmetric keys are protected by the public key, over all symmetric keys are deleted from the client. Encrypted data, keys are uploaded to the cloud. For downloading the data, client presents a policy file to cloud and downloads the encrypted ,decrypted data and keys. The FADE is a light-weight scalable method that give surety the deletion of files from cloud when requested by the user .during our examination 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 Semi-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 DaSCE is more secure than FADE when man-in-the-middle attack was introduced. DaSCE for out-sourced data to cloud that uses symmetric and asymmetric encryption combination .The DaSCE certify data confidentiality at a cloud as long as it is in use by the client. It also assures that data gets deleted it becomes not recoverable after deletes it from the cloud. Access control to both data, key through authority of guidelines and mutual authentication between client and key managers, cloud .Digital signatures and variation of Diffie-Hellman is used for common certification of arty. Successful authentication and session key concern amount produced in contact to asymmetric keys are mainly use in consequent cryptographic operations. The integrity of data for symmetric key and Message Authentication Code and securing symmetric keys to asymmetric keys generated by third party key managers.

II.RELATED WORKS

In This method provide a security to the cloud data in a number of service us, such as integrity, freshness, and availability. The authors in use a opening application in the organisation to handle the integrity and originality verify for the data. The Iris file system is planned to transfer association internal file system to the cloud[3]. A Merkle tree is used by gateway, which ensure originality and integrity of data by insert file blocks, MAC, and file version numbers at various levels of the tree. The gateway application maintain the cryptographic keys for confidentiality needs.

In proposed monitoring and auditing model that audits the cloud environment for ensuring the new data, data irretrievability, and resilience against disk failures. The methods depends on the user’s employed type for data confidentiality[7]. Data cannot be protected against service provider fully.

In the authors presented a cryptographic file method that provides confidentiality and integrity services to the outsourced data. The authors used hash based MAC tree for aforesaid services. Block-wise encryption is used for development of a MAC tree. The file salient side interacts with the file system of the server and outside of the encrypted blocks[4]. Encrypted file blocks and cryptographic metadata are stored individually. presence of cryptographic metadata on the storage side can be a prospective threat.

III.EXISTING METHOD

To provide the security for the data as well as Key maintenance in separate servers . Efficient method for the data storage in cloud environment. Authenticate the data owners and user requesting for downloading a file.

1.Cryptographic File System based on Hashed MAC:

Block-wise encryption is used for the construction of a MAC tree. The file system at the client side interacts with the file system of the server and outsources the encrypted blocks. Encrypted file blocks and cryptographic metadata are stored separately.

2. Cloud Storage System Based On Secure Erasure Code:

The system use verge key servers for storing a user’s key generated by a system manager. User encrypts the data divided into blocks and stores every block on randomly selected multiple servers.The system also provides the functionality of data transferred by allow any of the users to forward without downloading.

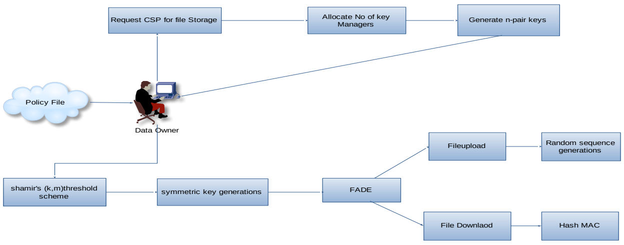
Request CSP for file Storage
Allocate No of key Managers
Generate n-pair keys
Policy File
Data Owner
Fileupload
Random sequence generations
shamir's (k,m)threshold scheme
symmetric key generations
FADE
File Downlaod
Hash MAC

Fig.1. Architecture of DASCE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

IV.PROPOSED WORK

The DaSCE use Shamir's k out of n threshold method to manage the keys, this will easy to generate the key. It uses multiple key managers, each represent one share of key.various key managers avoid single point of failure for the cryptographic keys. The FADE protocol provides privacy,security,integrity, access control, and guaranteed deletion to outsourcing data. The FADE uses both symmetric and asymmetric keys the client check the integrity of the folder. Symmetric decryption process is done by the user to retrieve the original data. DaSCE improved key management and authentication processes. secure group data sharing and forwarding The performance of the DaSCE is fast on the time consumption during file upload and File Download.Authentication is fully provided to all data located in public cloud.It takes relatively low cost.User selects their own number of key managers who are all needs to produce the key.Generally data owner generate the symmetric key value *S.* That will be spitted into k number of keys.Each key managers stores their key pair with its own identity and public key.

V.ALGORITHM

Digital Signature: Hash value of a significance when encrypted with the private key of a owner is his digital signature on that electronic Document.As the public key signer is agreed, anybody can check the message and the digital signature To provide accuracy ,reliability and Non denial to e-documents To use the Internet as the harmless and protected

Diffie-Hellman: The Diffie–Hellman key exchange technique allows two parties that have no previous information of each other together launch a collective secret key above an insecure channel. this key agreement provide varies authenticated protocols, and is also provide perfect self-assured defence in Transport Layer modes. it followed shortly by RSA

HMAC: A Hash Function produce a fingerprint of file, message, data protecting the integrity of a message validating it create a little fixed sized block.depending on both message checks it matches the MAC provide guarantee that communication is unchanged and comes from sender

FADE:
(a)File upload:

User access the constraint it is reachable in publically for establishing the session key,we are using the a primitive root and p is the large prime number.the client generates a random number calculate the session key by key manager .the file is uploaded based on the mod operation.the file upload process is multiple key manager.the interdependencies in file upload process is man in the middle attack

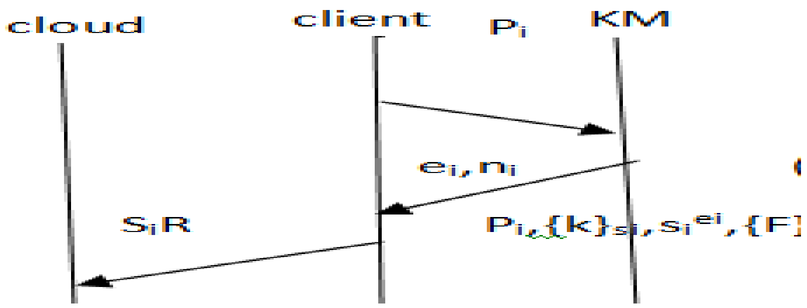

Fig.2. File Upload

DOI: 10.15680/IJIRCCE.2015. 0311154

(b)File download:

The client send requests to download the file after that encrypted keys in the cloud. The client check for the resoluteness of the file through the HMAC. Then the client generates a secret number and calculates sent to *KM* for decryption. The *KM* sends attributes used are based on *Pi*. The client extracts key from the received message and that in turn is used to decrypt *F*.

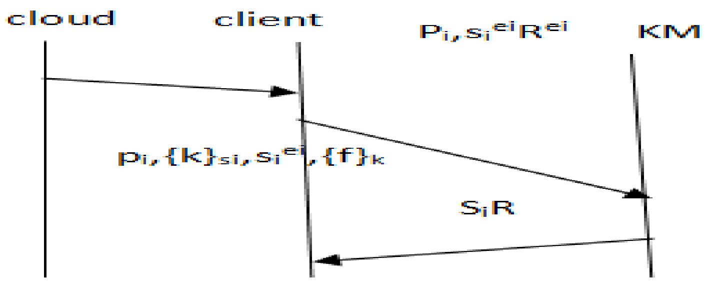

Fig.3. File Download

(c) Policy Revocation:

The client send a request to the key manager for revoke the file. The key manager provide a random number and send it to the client for decryption process. The authentic client decrypts *r*, calculates the hash value,and sends it backward to the key manager. After that key verification, the *KM* revokes policy file and acknowledge

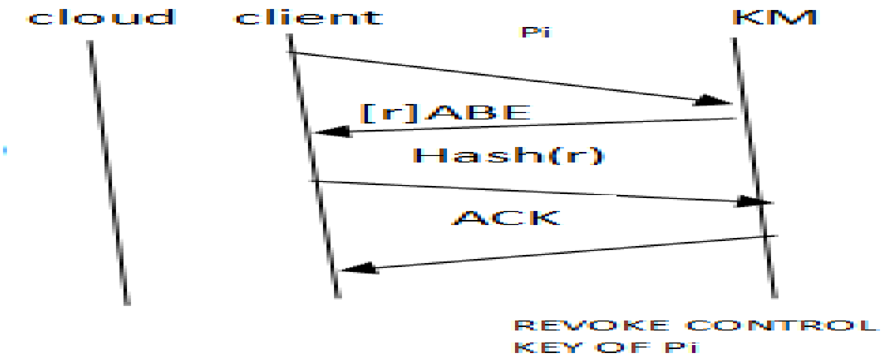

Fig.4. Policy Revocation

(D) Policy Renewal:

If policy file *pi is* needs to be renewed as *Pj*, client download the file and send it to the key manager it is encrypted by the Si after that decrypted by Pj, *KM* sends new public key parameters(*ej*, *nj*) to client as now formally analyze FADE it is renewal by the key manager

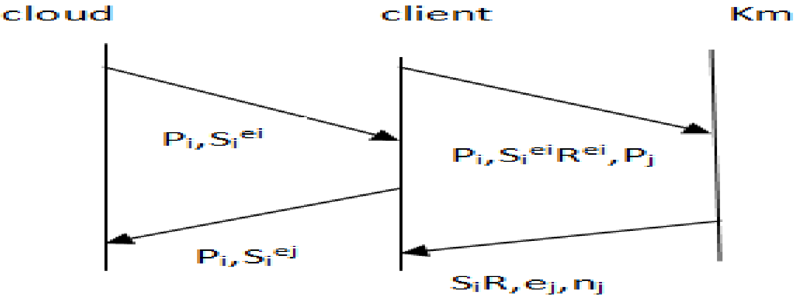

Fig. 5. Policy Revocation

VI.MODULE DESCRIPTION

(1)Key manager setup:

For the efficient storage of different keys to encrypt the file which could be stored in cloud, needs key managers. All the key managers are authenticated by the cloud service provider .Each manager has its own identity and generate the key for encrypt the file.

(2)Keys for file encryption:

User selects their own number of key managers who are all needs to produce the key.Generally data owner generate the symmetric key value *S.* That will be spitted into k number of keys.Each key managers stores their key pair with its own identity and public key.

(3) Shamir's Strategy:

Help to reconstruct the symmetric key *s*, by getting many parts of key from specified key managers. Here k represent the number of key managers and n represents spited number of symmetric keys on all key managers(km)client :breaks up symmetric keys s into n shares(s1,s2,sn).encrypt i th shares with the public keys of i th km. upload all shares of s to cloud. client downloads all shares of key client selects k number of kms randomly.sends i th share of s to its km. receives back decrypted i th share. reconstructs s from k shares according to Shamir's strategy

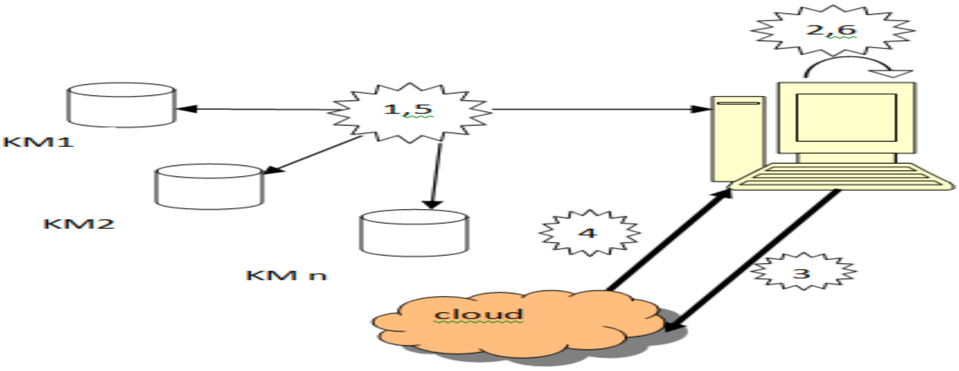

Fig. 6.Shamir's Strategy

VII.CONCLUSION

Proposed the DaSCE protocol, a cloud storage security system that provided key management, access control, and file assured deletion for group data sharing and forwarding. Assured deletion is mainly depends upon the policy file encrypted and upload. On revocation of policies, access keys are deleted by the *KMs* that result in halting of the contact to the data the files be reasonably deleted from the cloud. The key management mainly using (*k*, *n*) threshold secret sharing mechanism for complete the task We analyzed and model FADE by using the operating of file upload and file download. Some uses are highlighted in the FADE . DaSCE improved key authentication and management process the presentation and efficient of the DaSCE was evaluate depends on the time consumption during file upload and download. The results base on that the DaSCE protocol can be practically used for clouds for security of outsourced information .The reality that the DaSCE does not want any protocol and implementation level changes at the cloud makes it highly practical methodology for cloud.

REFERENCES

1. C. de Morais Cordeiro, H. Gossain, and P. Agrawal, “Multicast over wireless mobile ad hoc networks: Present and future directions,” IEEENetw., vol. 17, no. 1, pp. 52–59, Jan./Feb. 2003.
2. W. Liao and M.-Y. Jiang, “Family ACK tree (FAT): Supporting reliable multicast in mobile ad hoc networks,” IEEE Trans. Veh. Technol., vol. 52,no. 6, pp. 1675–1685, Nov. 2003.
3. G. Ateniese, M. Steiner, and G. Tsudik, “New multi-party authentication services and key agreement protocols,” IEEE J. Sel. Areas Cmmun, vol. 18, no. 4, pp. 628–639, Apr. 2000.
4. M. Steiner, G. Tsudik, and M. Waidner, “Key agreement in dynamic peer groups,” IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769–780 Aug. 2000.
5. Y. Kim, A. Perrig, and G. Tsudik, “Simple and fault-tolerant key agreement for dynamic collaborative groups,” in Proc. ACM Conf. Comput .Commun. Security, Nov. 2000, pp. 235–244. [3] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2,pp. 743–754, Apr. 2012.
6. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1,pp. 131–143, Jan. 2013.
7. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, “SecurelyOutsourcing attribute-based encryption with check ability,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 8, pp. 2201–2210Aug. 2014.
8. P. Barralon, N. Vuillerme, and N. Noury, “Walk detection with a kinematic sensor: Frequency and wavelet comparison,” in EMBS’06. IEEE, 2006, pp. 1711–1714.
9. H. Wang, S. Sen, A. Elgohary, M. Farid, M. Youssef, and R. R.Choudhury, “No need to war-drive: Unsupervised indoor localization,”10th Mobisys. ACM, 2012, pp. 197–210.