Secure Data Access Privacy Preserving using Cloud Services

M. Suguna, D. Prakash, Cynthia. J

Abstract: In spite of the tremendous computationaladvantages, outsourcing data to the public cloud is also preventing customers' direct control over the systems that use their data, which unavoidably brings in new security challenges. Cloud computing gives numerous advantages and unparalleled convenience for the cloud customers to get the on-demand access of cloud provided that the local infrastructure limitations need not be taken into account. While accessing data, there may be a co-operative relationship among different users which makes sharing and exchanging of information, a tedious process. The view of current security solutions is mainly on authentication to apprehend that the data of an individual cannot be approached illegally, but there arose a privacy issue when a user request for data sharing to other users through cloud server. The users' privacy may be exposed by challenged access request itself regardless of whether the data access permission for the user is obtained or not. In the proposed system, a privacy-preserving authentication protocol is employed to prevent the above privacy complications. In this technique, authority of data through shared access is achieved by the process of sending anonymous access request which gives privacy to the cloud users. Access control is based on attributes so that the cloud users can only access their own authorized data fields. Advanced encryption standard algorithm is used to achieve data anonymity and data protection. The proposed method dealt with secure privacy preserving data access authority is attractive for multiple-user in cloud real time storage.

Index Terms: Cloud computing, authentication protocol,shared authority, privacy preservation, data anonymity.

I. INTRODUCTION

The venture of cloud computing provides a significant Progress in the field of IT industry. It is one of the mostpromising technologies out in the world today which gives numerous benefits to any organization or an individual. It comes with more appealing data storage, on-demand services, ubiquitous network access and convenient data exchange for the users. Cloud computing offers solutions for data storage irrespective of local infrastructure limitations as well as equips the users with a platform to process their information. The main focus of this technology is to widen the efficacy of shared resources available in the cloud and also to reallocate them dynamically if needed.Even though the technology provides endless benefits, it lacks tight security capabilities and creates privacy issues for the data owners. Traditional security measures primarily relate to authentication of users to apprehend that the users access their own data fields. Along with the issues regarding security, there arose other issues when the cloud users need to share and access each other's authorized information to bring about tremendous benefits.

An example is considered where a group of supplier, carrier and retailer takes part in the system. Each group has its own set of authorized information and has access permission to access their data. In accessing data from different group privacy is revealed during the access request itself which becomes a security issue here. So, anonymous request matching mechanism is used to protect the privacy of the users. Different access control for different group of users is provided by a trusted third party auditor.

II. RELATED WORK

Numerous schemes making use of attribute based encryption for access control of outsourcedinformation in cloud computing. The limelight of currentsecurity solutions is mainly on authentication to apprehend that the data of an individual cannot be approached illegally, but there arose a privacy issue when a user request for data sharing to other users through cloud server.

A multi owner data sharing secure scheme (Mona) has been proposed for dynamic groups in the cloud applications. The Mona ensures the users that they can securely share their data with other users through several untrusted cloud servers. Here, a new user can access the data files without the knowledge of data owners. Any user in the group can access and utilize the resources anonymously.

Later, Zero knowledge proof (ZKP) based authentication scheme have been proposed for cloud services. In home networks, the approach is usually user centric which allows sharing of personal data that is based TCP/IP framework where a trusted third party is introduced for decentralized interactions. A broadcast group key management (BGKM) is used to better the delicacy of symmetric key cryptosystem in public clouds. Attribute based access control method is used so that the contents can be decrypted by a user provided the identity attributes matches with the data owner's policies. There is an apparent advantage of BGKM when adding/revoking users and updating access control policies.

Provable data possession and proofs of retrieve ability have been proposed to verify data availability and integrity in cloud storages. Lightweight PDP scheme depends on cryptographic hash function and symmetric key encryption was also proposed yet due to the lack of randomness in the challenges servers can cheat the owners by using previous metadata. Cloud storage is an emerging technology which faces problem in security such as data confidentiality, integrity, and availability.

Revised Version Manuscript Received 25 November, 2018

M.Suguna, Assistant Professor-II, Department of CSE, Kumaraguru College of Technology, Coimbatore (Tamil Nadu), India.

D. Prakash, Assistant Professor, EEE Department, SREC, Coimbatore (Tamil Nadu), India.

Cynthia. J, Professor, CSE Department, Kumaraguru College of Technology, Coimbatore (Tamil Nadu), India.

Designated Verifier Provable Data Possession (DV-PDP) scheme design depends on ECC-based homomorphism authenticator. Costly bilinear computing is removed in this scheme. This design has PDP properties such as stateless cloud storage and verifier independent. This design is proved to be secure and efficient by security analysis and performance analysis. DV-PDP contains a trusted third party for checking data integrity with permission from its owner. Here, verifier requires extra setup and client performs extra computation. Complexity is increased due to pairing based approach.

A number of security issues were labeled in the preceding works. Yet a user's privacy is revealed by access request itself as a result of requesting data from the cloud server has not been studied. Here, we tend to recognize a new privacy challenge and propose a protocol not solely to concentrate on authentication that validates the information fields of approved users, however conjointly to supply the privacy protective access.

III. SYSTEM MODEL

Fig. 1 demonstrates a system model for the cloud storage architecture where users, cloud server and a trusted third party are the three main network entities.

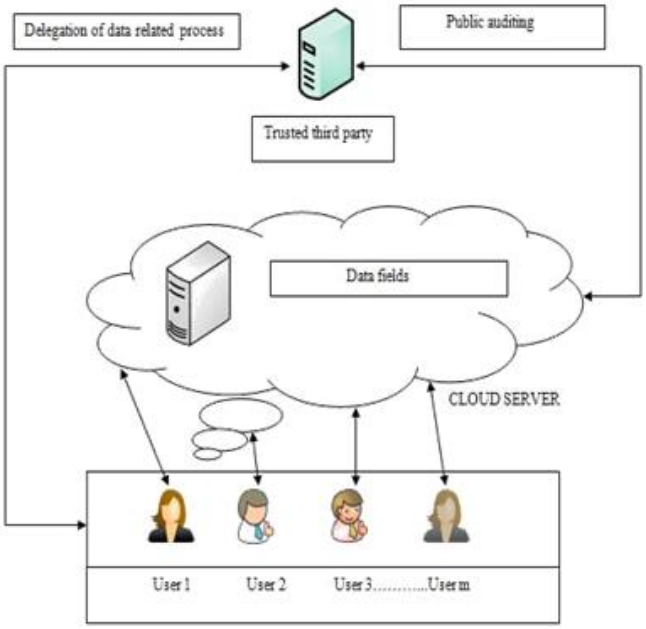

Fig. 1. System Model for Cloud Storage

User: A user may be an individual or an organization that outsourced their data to the public cloud for computing. Different users may be in a collaborative relationship and each of them has their own set of authorized data fields. In the proposed system the user may a supplier or a retailer. Supplier is the one who uploads their data in the cloud storage which gets stored in the cloud in encrypted form. Retailer is the person who requests the data from the cloud storage for their personal computing.

Cloud server: A cloud server is a cloud storage provider that supplies cloud storage and computing facilities to the users. The cloud server is considered as a system which provides enormous amount of storage and resources for the cloud users. A user has to get registered in the cloud server to store or exchange data in the cloud space.

Trusted third party: It is a neutral entity which audits the data in the cloud storage on behalf of all the registered users. It provided keys to the retailers to decrypt the data downloaded from the cloud space.

IV. PROPOSED SYSTEM DESCRIPTION

A privacy-preserving authentication protocol is employed in the system to prevent the above privacy complications. In this technique, authority of data through shared access is achieved by the process of sending anonymous access request which gives privacy to the cloud users. Access control is based on attributes so that the cloud users can only access their own authorized data fields. Advanced Encryption Standard (AES) algorithm is used to achieve data anonymity and data protection. This method access authority is enticing for multiple-user cloud applications.

Cloud computing has great capability which provides the customers strong computational power at less cost. The customers with limited computing resources can economically enjoy the computing power, mass storage and bandwidth by outsourcing their data to the cloud. Even software can be shared in a pay-per-use manner through cloud computing technology. Thus the feature of outsourcing data is regarded as a fundamental benefit of the cloud paradigm.

However, the outsourced information may consist of sensitive data such as business related information, personal medical data, health records, employee information, research theories, etc. The amount of crucial information available in the internet is getting increased every day, so the need to keep away the unauthorized users from illegal access of data becomes apparent. With the current computing technologies, stealing someone's data is unchallenged as it can be achieved without much effort. Thus certain verification techniques have to be considered to know whether the person is authorized or not. Unauthorized leakstorage of information should be prevented by encrencrypting the data before uploading to cloud.

The proposed work involves the following. Users who are participating in the cloud need to register their personal details. These details include their name, address, email id, password, and gender. After the verification of cloud storage provider, every user gets unique private key or ID to access the cloud storage. These private keys are sent to the email id of the respective individuals secretly. Cloud storage provider provides the cloud space to the users to upload and download the files in the storage. Cloud storage provider maintains the entire details of the users involving in the cloud. Users can login the cloud with the presence of private key with their respective username and password.

Every user can login to the system with the respective email id, password and private key. Users can upload the files in the cloud storage. These files are stored in the cloud in encrypted form. Advanced encryption standard algorithm is used to encrypt the data in the cloud. If any chance of hacking done during the transfer hacker cannot view the content, because secret key is set to the encrypted file.

Fig.2. represents the auditing of cloud storage. If a user wants to download contents from the cloud, the user has to request the trusted third party auditor to send the key to decrypt the file. The trusted third party auditor verifies the requested users and takes decisions to send the key or to ignore the user. Here, even when the requested data is not provided, the privacy that what data the person needs is concealed. The access request is anonymous which helps to protect the users' privacy even in the case of denial of data access. Also, the proposed scheme helps the users to access the cloud storage with easy communication and less computing cost.

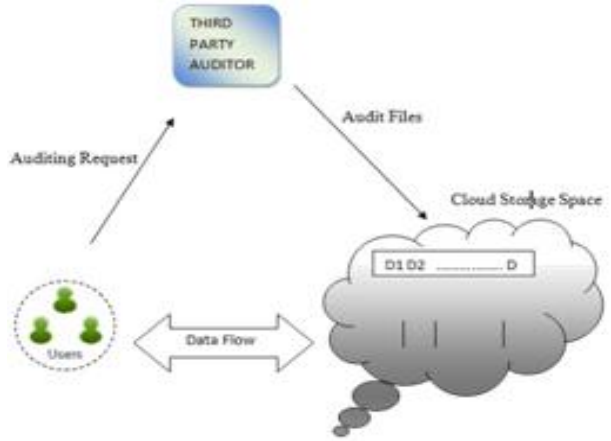

Fig. 2. Auditing the Cloud Storage.

V. E-R DIAGRAM

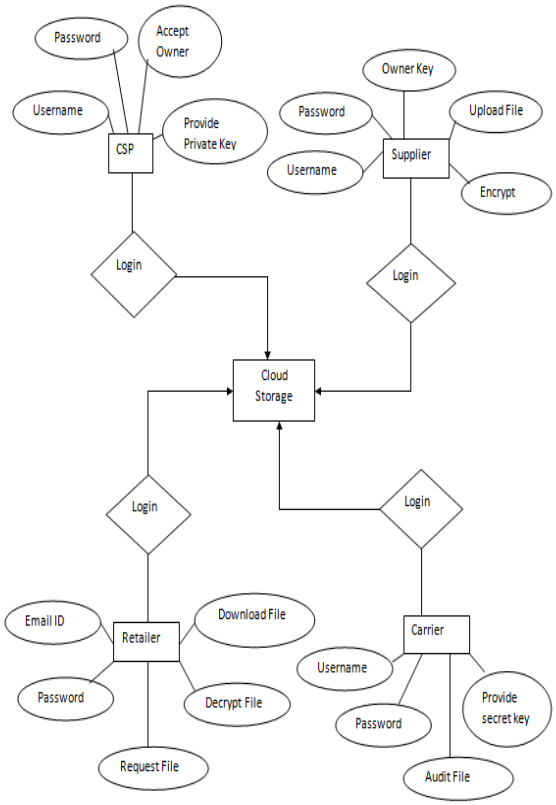

Fig. 3.E.R Diagram of Proposed work

The above Fig.3 represents the actions performed by Cloud Service Provider, retailer, carrier and supplier.

Retailer can request for files, download files, read files. Supplier can upload, download, modify and store file in cloud. The files uploaded by other users can also be downloaded by supplier. Cloud storage provider provides space to suppliers on cloud after registration. Carrier can view supplier files, audit files, provide access rights to suppliers and retailers.

VI. MODULE DESCRIPTION

A. Registering A Supplier

Suppliers who are participating in the cloud need to register their personal details. These details include their name, address, email id, password, and gender. Once registered, the login request is sent to the CSP. After the verification of cloud storage provider, every supplier gets private key to access the cloud storage. These private keys can send to the supplier individual mail id secretly.

The private key is generated by the random generator when the cloud storage provider accepts the login request. The supplier needs to enter the private key every time when they login to the cloud. The supplier can upload the files in different category like drama, adventure, medicine, science, etc. The supplier also has the authority to delete own files from the cloud. The supplier can search files in the cloud and also can request files uploaded by others.

B. Providing Cloud Space

Cloud storage provider provides the cloud space to the suppliers to upload the files in the storage. CSP maintain the entire details. CSP provide the private keys to the suppliers. After the verification of CSP only suppliers can upload the files in the cloud. Supplier can login the cloud with the presence of private key.

C. Encrypting The Uploaded Files

Every supplier can login to the system with the respective email id, password and private key. Supplier can upload the files in the cloud storage. These files are stored in the cloud in encrypted form. Advanced encryption standard algorithm is used to encrypt the data in the cloud. If any chance of hacking done during the transfer hacker cannot view the content, because the files are encrypted and decrypted using AES algorithm.

D. Requesting Files From Cloud

Retailer can use the files that are uploaded in the cloud. Retailer must register with their details. Retailer can login to the cloud with the respective username and password. Before downloading the file from the cloud, retailer must send the request to the trusted third party auditor for the secret key to decrypt the files.

E. Auditing The Files

Trusted third party auditor or carrier audits all the files that are uploaded in the cloud storage without viewing the content of the file. If any of the file requested from the retailer, supplier cannot send the secret key directly to the retailer. It will send to the carrier to verify the file.

F. Downloading From Cloud

Retailer cannot download the file without the permission of carrier.

In this module, after the carrier verification, secret key is send to the requested retailer. Retailer can decrypt the file and download the file only if the secret key of the file matches.

VII. CONCLUSION

In this work, a new privacy issue is identified while accessing data in the cloud. Authentication protocol is employed to assure data confidentiality and integrity. Data anonymity is established by wrapping the data while transmitting them. Privacy preserving technique is used to prevent the exposure of users' privacy while challenging access request. Access request is anonymous which secretly informs the server about the users' desired data.

Thus, the proposed scheme is very likely to be applied for privacy preservation in cloud related applications.

REFERENCES

1. K. Yang and X. Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp.1717 -1726, 2013.
2. M. Nabeel , N. Shang and E. Bertino "Privacy Preserving Policy Based Content Sharing in Public Clouds", IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp.2602 -2614, 2013
3. S. Sundareswaran , A.C. Squicciarini and D. Lin "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp.556 -568, 2012
4. H. Wang "Proxy Provable Data Possession in Public Clouds", IEEE Trans. Services Computing, vol. 6, no. 4, pp.551 -559, 2012
5. Q. Wang , C. Wang , K. Ren , W. Lou and J. Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp.847-859 -25, 2011
6. L.A. Dunning and R. Kresman "Privacy Preserving Data Sharing with Anonymous ID Assignment", IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp.402 -413, 2013
7. C. Wang , Q. Wang , K. Ren , N. Cao and W. Lou "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Services Computing, vol. 5, no. 2, pp.220 -232, 2012
8. Y. Tang , P.C. Lee , J.C.S. Lui and R. Perlman "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Trans. Dependable and Secure Computing, vol. 9, no. 6, pp.903 -916, 2012
9. S. Ruj , M. Stojmenovic and A. Nayak "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds", IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp.384 -394, 2014
10. J. Chen , Y. Wang and X. Wang "On-Demand Security Architecture for Cloud Computing", Computer, vol. 45, no. 7, pp.73 -78, 2012
11. Y. Zhu , H. Hu , G. Ahn and M. Yu "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp.2231 -2244, 2012
12. X. Liu , Y. Zhang , B. Wang and J. Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp.1182 - 1191, 2013.