International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

An Approach for Preserving Privacy of Shared Data in the Cloud

*R.BHARATH **E.PRAVEEN

*M.TECH student, Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING
**Assistant Professor, Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING

ABSTRACT

Cloud computing is transpire as a prevalent data interactive paradigm to perceive user data remotely stored in an online cloud server. Cloud services furnish great conveniences for the users to enjoy the on-demand cloud applications without contemplating the local infrastructure limitations. During the information accessing, several users may be in collective relationship, and thus information sharing becomes consequential to achieve productive benefits. The existing security solutions mainly concentrate on the authentication to notice the user's privative information cannot be unauthorized accessed, but precise privacy problem during a user challenging the cloud server to appeal other users for information sharing. The challenged access invocation itself may reveal the users privacy no matter whether or not it can be acquire the information access permissions. In this paper, we introduced shared authority based privacy preserving authentication protocol to address above privacy problem for cloud storage. In this shared authority based privacy preserving authentication, 1) shared access authority attained by unknown access request matching procedure with security and privacy considerations.; 2) attribute based access command is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to furnish information distribution among the multiple users. Meantime, global computability model is established to demonstrate that the SASP theoretically has the design correctness. It designate that the proposed protocol perceiving privacy preserving information access authority sharing is attractive for multi user collaborative cloud applications.

I. INTRODUCTION

Cloud computing is optimistic information technology architecture for both enterprises and individuals. It introduces an attractive data storage and interactive pattern with prominent advantages, including on-demand self-services, omnipresent network access, and location individualistic resource pooling. Towards the distributed computing, a common administration structural engineering is anything as an administration, in which foundations, stage, programming, and others are connected for pervasive interconnections. Late studies have been attempted to advance the distributed computing advance towards the web of administrations. Eventually, security and privacy issues are becoming key concerns with the increasing popularity of cloud services. Customary security approaches chiefly concentrate on the solid validation to understand that a client can remotely get to its own particular information in on-interest mode. Alongside the differences of the application prerequisites, clients might need to get to and share one another's approved information fields to accomplish profitable benefits, which brings new security and protection challenges for the distributed storage. A case is acquainted with distinguish the principle inspiration. In the distributed storage based production network administration, there are different vested parties (e.g., supplier, transporter, and retailer) in the framework. Every gathering claims its clients which are allowed to get to the approved information fields, and distinctive clients own generally free get to powers. It implies that any two clients from various gatherings ought to get to distinctive information fields of the same file. There into, a supplier intentionally might need to get to a transporter's information fields, however it is not certain whether the bearer will permit its entrance demand. On the off chance that the transporter rejects its demand, the supplier's entrance craving will be uncovered alongside nothing acquired towards the wanted information fields. Really, the supplier may not send the entrance ask for or pull back the unaccepted solicitation ahead of time on the off chance that it firmly realizes that its solicitation will be rejected by the transporter. It is outlandish to completely reveal the supplier's private data with no security contemplations.

- **Case 1:** The carrier additionally needs to get to the supplier's information fields, and the cloud server ought to illuminate one another and transmit the mutual access power to the both clients.

- **Case 2:** The carrier has no enthusiasm on other clients' information fields, along these lines its approved information fields ought to be appropriately secured, then the supplier's entrance solicitation will likewise be dissembled.

- **Case 3:** The carrier might need to get to the retailer's information fields, yet it is not sure whether the retailer will acknowledge its solicitation or not. The retailer's approved information fields ought not be open if the retailer has no hobbies in the carriers information fields, and the bearer's solicitation is likewise secretly hidden.

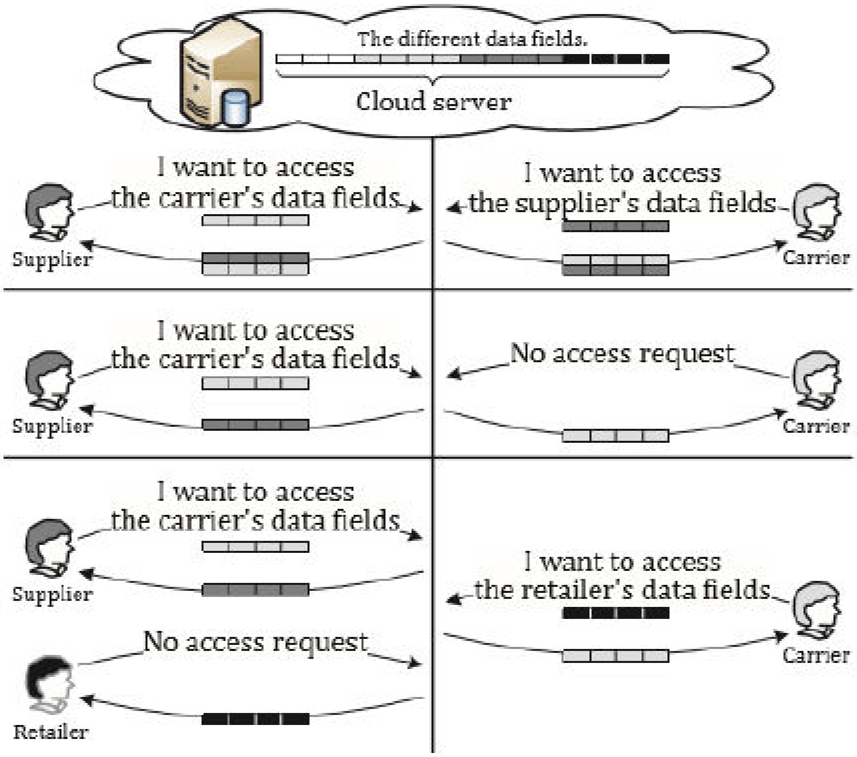
The different data fields.
Cloud server
I want to access the carrier's data fields
Supplier
I want to access the supplier's data fields
Carrier
I want to access the carrier's data fields
Supplier
No access request
Carrier
I want to access the carrier's data fields
Supplier
No access request
Retailer
I want to access the retailer's data fields
Carrier

Fig.1. Three Possible Cases During Data Accessing and Data Sharing in Cloud Applications

From above three cases, security protection and privacy preservation are both contemplate without disclosing sensitive access desire related data. In the cloud environments, a rational security protocol should attain the following requirements.

1) Authentication: a legal user can access its individual data fields, only the authorized limited or entire data fields can be identified by the judicial user, and any forged or tampered data fields cannot deceive the judicial user.

2) Data anonymity: any unrelated entity cannot recognize the exchanged data and communication state even it intercept the exchanged messages via an open medium.

3) User privacy: any unrelated entity cannot know or guess a user's access desire, which illustrate a user's interest in another user's authorized data fields. If and only if the both users have correlative interests in each other's authorized data fields, the cloud server will notify the two users to perceive the access permission sharing.

4) Forward security: any opponent cannot correspond two communication sessions to derive the earlier interrogations according to the currently captured messages. In this paper, we notify the preceding privacy problem to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud information storage, which discern authentication and authorization without compromising a user's private information. The main offerings are as follows. 1) Distinguish a new privacy challenge in cloud storage, and address a subtle privacy problem during a user challenging the cloud server for information sharing, in which the challenged request itself cannot reveal the user's privacy not important whether or not it can obtain the access authority. 2) Propose an authentication protocol to improve a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching method. 3) Apply ciphertext-policy attribute based access control to perceive that a user can reliably access its own information fields, and acquire the proxy re-encryption to provide temp authorized data sharing among various users.

II. RELATED WORK

In this we presented an unknown ID task based information sharing calculation for multiparty situated cloud and conveyed figuring frameworks. In the AIDA, a whole number information sharing calculation is planned on top of secure aggregate information mining operation, and receives a variable and unbounded number of emphases for mysterious task. Especially, Newton's characters and Sturm's hypothesis are utilized for the information mining, a dispersed arrangement of specific polynomials over finite fields improves the calculation versatility, and Markov fasten representations are utilized to decide measurements on the required number of cycles. We proposed a multi-proprietor information sharing secure plan for element bunches in the cloud applications. The Mona expects to understand that a client can safely impart its information to different clients by means of the un trusted cloud server, and can productively bolster element bunch collaborations. In the plan, another allowed client can specifically decode information files without pre-reaching with information proprietors, and client disavowal is accomplished by a denial list without upgrading the mystery keys of the remaining clients. Access control is connected to guarantee that any client in a gathering can secretly use the cloud assets, and the information proprietors' genuine personalities must be uncovered by the gathering administrator for question assertion. It demonstrates the capacity overhead and encryption calculation expense are autonomous with the measure of the clients. We proposed a zero-information evidence (ZKP) based validation plan for sharing cloud administrations. In light of the social home systems, a client driven methodology is connected to empower the sharing of customized substance and refined system based administrations through TCP/IP foundations, in which a trusted outsider is presented for decentralized associations. We proposed abroad cast gathering key administration (BGKM) to enhance the shortcoming of symmetric key cryptosystem in broad daylight mists, and the BGKM understands that a client need not use open key cryptography, and can progressively infer the symmetric keys amid decoding. As needs be, quality based access control instrument is intended to accomplish that a client can unscramble the substance if and just if its character properties fulfill the substance supplier's arrangements. The fine-grained calculation applies access control vector (ACV) for allocating insider facts to clients taking into account the character characteristics, and permitting the clients to determine genuine symmetric keys in view of their privileged insights and other open data. The BGKM has a conspicuous point of interest amid including/renouncing clients and overhauling access control strategies. We proposed a disseminated stockpiling honesty inspecting component, which presents the homomorphic token and conveyed deletion coded information to upgrade secure and tried and true stockpiling administrations in distributed computing. The plan permits clients to review the distributed storage with lightweight correspondence over-burdens and calculation expense, and the inspecting result guarantees solid distributed storage accuracy and quick information blunder confinement. Towards the dynamic cloud information, the plan underpins element outsourced information operations. It demonstrates that the plan is flexible against Byzantine disappointment, noxious information modification assault, and server intriguing assaults. We built up a decentralized data responsibility structure to track the clients' real information utilization in the cloud, and proposed an item focused way to deal with empower encasing the logging instrument with the clients' information and strategies. The Java Archives (JAR) programmable ability is utilized to make a dynamic and portable article, and to guarantee that the clients' information access will dispatch validation. Moreover, appropriated examining instruments are additionally given to fortify client's information control, and tests exhibit the methodology productivity and effectiveness.

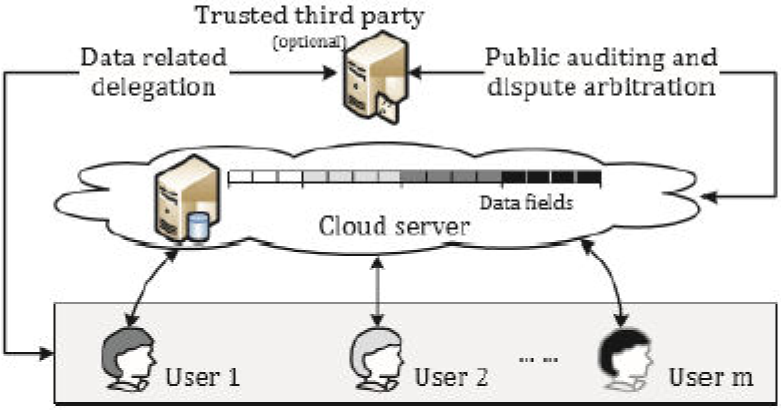

Fig: The Cloud Storage System Model

In the previously stated works, different security issues are tended to. Be that as it may, a client's inconspicuous access solicitation related security issue created by information getting to and information sharing has not been concentrated yet in the writing. Here, we distinguish another security challenge, and propose a convention not just concentrating on validation to understand the substantial information getting to, additionally considering approval to give the protection safeguarding access power sharing. The characteristic based access control and intermediary re-encryption components are together connected for validation and approval.

III. SYSTEM MODEL

Above fig illustrates a system model for the cloud storage architecture, which includes three main network entities: users (Ux), a cloud server (S), and a trusted third party.

• **User:** an individual or group entity, which owns its information stored in the cloud for online information storage and computing. Different users may be belongs to a common organization, and are allocated with independent authorities on specific data fields.

• **Cloud server:** an entity, which is controlled by a specific cloud service provider or cloud application operator to provide information storage and computing services. The cloud server is regarded as an entity with unrestrained storage and computational resources.

• **Trusted third party:** an elective and neutral entity, which has enhanced capabilities on behalf of the users, to accomplish data public auditing and dispute arbitration. In the cloud storage, a user stores his data remotely via online procedure and software for cloud services, which are operated in the distributed, parallel, and cooperative modes. In the distributed storage, a client remotely stores its information by means of online foundations, flatforms, or programming for cloud administrations, which are worked in the conveyed, parallel, and helpful modes. Amid cloud information getting to, the client self-governingly cooperates with the cloud server without outer obstructions, and is doled out with the full and autonomous power all alone information fields. It is important to ensure that the clients' outsourced information can't be unapproved gotten to by different clients, and is of basic significance to guarantee the private data amid the clients' information access challenges. In a few situations, there are numerous clients in a framework (e.g., store network administration), and the clients could have distinctive affiliation characteristics from diverse vested parties. One of the clients might need to get to other partner clients' information fields to accomplish bi-directional information sharing, yet it thinks about two angles: whether the pointed client might want to share its information fields, and how can't uncover its entrance demand if the pointed client decays or overlooks its test. In the paper, we give careful consideration on the procedure of information access control and get to power sharing other than the specific file situated cloud information transmission and management.

IV. CONCLUSION

In this paper, we have recognized a new privacy challenge during data accessing in the cloud computing to attain privacy-preserving access authority sharing. Authentication is entrenched to guarantee data confidentiality and data integrity. Data inconspicuousness is achieved since the wrapped values are interchanged during transmission. User privacy is improved by anonymous access requests to privately notify the cloud server about the users' access interests. Forward security is perceived by the session determiner to prevent the session correlation. It demonstrates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

[1] P. Mell and T. Grance, “Draft NIST Working Definition of Cloud Computing,” National Institute of Standards and Technology, USA, 2009.

[2] A. Mishra, R. Jain, and A. Durresi, “Cloud Computing: Networking and Communication Challenges,” IEEE Communications Magazine, vol. 50, no. 9, pp, 24-25, 2012.

[3] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, “Key Challenges in Cloud Computing to Enable the Future Internet of Services,” IEEE Internet Computing, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, 2012.

[4] K. Hwang and D. Li, “Trusted Cloud Computing with Secure Resources and Data Coloring,” IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.

[5] J. Chen, Y. Wang, and X. Wang, “On-Demand Security Architecture for Cloud Computing,” Computer, vol. 45, no. 7, pp. 73-78, 2012.

[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, “Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, “Proxy Provable Data Possession in Public Clouds,” IEEE Transactions on Services Computing, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[8] K. Yang and X. Jia, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing,” IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on

Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[10] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, 2010.

[11] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[12] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.

[13] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, 2011.

[14] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.

[15] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.

[16] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.

[17] Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 903-916, 2012.

[18] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, "Towards Temporal Access

Control in Cloud Computing," in Proceedings of the 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012), pp. 2576-2580, March 25-30, 2012.

[19] S.Ruj,M.Stojmenovic,andA.Nayak,"DecentralizedAccessControl with Anonymous Authentication for Securing Data in Clouds," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6463404, 2013.

AUTHOR 1 :-
*R. Bharath completed his B tech in Balaji Institute of Technology & Science in 2014 and pursuing M-Tech in Vaagdevi College of Engineering
AUTHOR 2:-
**E. Praveen is working as Assistant Professor in Dept of CSE, Vaagdevi College of Engineering