ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Accessing and Sharing Using SAPA Protocol in Cloud Computing

K.Siva Prasad
Dept of Software Engineering,
SKR College of Engineering and Technology,
Nh-5, Kondurusatram, Manubolu,
SPSR Nellore, Ap.

Syed Baji, Ph.D
Associate Professor,
Dept of Software Engineering,
SKR College of Engineering and Technology,
Nh-5, Kondurusatram, Manubolu,
SPSR Nellore, Ap.

Abstract:

Cloud computing is continuously developing as a standard for sharing the data over the remote storage in an online cloud server. Cloud services offers great amenities for the users to enjoy the on-demand cloud applications without any obligations related to data. During the data retrieving, different users may be in a cooperative relationship, and hence data distribution becomes important. Though the user's data is not accessed by unwanted sources, the other's data is exposed to risk by request for sharing The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose mutual authority using privacy preserving and authentication protocol or in other word a shared authority using privacy preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control 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 provide data sharing among the multiple users. Meanwhile, universal compos ability (UC) model is established to prove that the mutual authority using privacy preserving and authentication protocol theoretically has the design correctness. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing, is attractive for multi-user collaborative cloud applications.

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

INTRODUCTION:

Cloud computing is that the delivery of computing and storage capability as a service to a heterogeneous community of end-recipients. Cloud computing could be a general term for love or money that involves delivering hosted services over the web. A model for delivering data technology services during which resources square measure retrieved from the web through web-based tools and applications. Cloud computing is therefore named as a result of the knowledge being accessed is found within the "clouds", and doesn't need a user to be in an exceedingly specific place to achieve access to that. Cloud computing refers to applications and services offered over the web. These services square measure offered from information centers everywhere the planet, that jointly square measure brought up because the "cloud." the thought of the "cloud" simplifies the numerous network connections and laptop systems concerned in on-line services. Cloud computing is computing model, not a technology. during this model of computing, all the servers, networks, applications and different parts associated with information centers square measure created offered to that and finish users. Cloud computing could be a form of computing that's cherish grid computing. It depends on sharing computing resources instead of having native servers or personal devices to handle applications. Software as a service: Saas has become a typical delivery model for many business applications, along with accounting, collaboration, shopper relationship management (CRM), management information systems. Platform as a service: It is a class of cloud computing services that offer a computing platform and an answer stack as a service. along side SaaS and IaaS, it's a service model of cloud computing.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Infrastructure as a service: IaaS refers to not a machine that will all the work, however merely to a facility given to businesses that provides users the leverage of additional space for storing in servers and knowledge centers. In this paper we have discussed about the related work, the proposed work, the architectural diagram, the modules present in the paper, the algorithm used to implement the idea and its application in the near future.

The main contributions are as follows:

1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.

2) Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.

3) Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users. The remainder of the paper is organized as follows. Section 2 introduces related works. Section 3 introduces the system model, and Section 4 presents the proposed authentication protocol.

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy in company strength. Once these things are satisfied, then next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites .“Privacy Preserving Data Sharing with Anonymous ID Assignment,”: We proposed an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty oriented cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed on top of secure sum data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem are used for the data mining, a distributed solution of certain polynomials over finite fields enhances the algorithm scalability, and Markov chain representations are used to determine statistics on the required number of iterations. “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud”: We consider a multi-owner data sharing secure scheme (Mona) for dynamic groups in the cloud applications. The Mona aims to realize that a user can securely share its data with other users via the untrusted cloud server, and can efficiently support dynamic group interactions.

In the scheme, a new granted user can directly decrypt data files without pre-contacting with data owners, and user revocation is achieved by a revocation list without updating the secret keys of the remaining users. Access control is applied to ensure that any user in a group can anonymously utilize the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration. It indicates the storage overhead and encryption computation costar independent with the amount of the users.

“Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking,”: We proposed a zero-knowledge proof (ZKP) based authentication scheme for sharing cloud services. Based on the social home networks, a user centric approach is applied to enable the sharing of personalized content and sophisticated network-based services via TCP/IP infrastructures, in which a trusted third party is introduced for decentralized interactions. “Privacy Preserving Policy Based Content Sharing in Public Clouds”:

We proposed a broadcast group key management (BGKM) to improve the weakness of symmetric key cryptosystem in public clouds, and the BGKM realizes that a user need not utilize public key cryptography, and can dynamically derive the symmetric keys during decryption. Accordingly, attribute based access control mechanism is designed to achieve that a user can decrypt the contents if and only if its identity attributes satisfy the content provider's policies. The fine-grained algorithm applies access control vector (ACV) for assigning secrets to users based on the identity attributes, and allowing the users to derive actual symmetric keys based on their secrets and other public information.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

PROBLEM STATEMENT:

The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may expose the user's privacy no matter whether or not it can obtain the data access permissions. Existing data reduplication systems, the cloud is occupied as a different to allow data owner/ users to securely perform duplicate check with differential privileges. The data owners only outsource their data storage by utilizing cloud.

Disadvantages:

During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions.

PROBLEM SOLUTION:

In this project, we propose a mutual or shared authority using privacy-preserving and authentication protocol (SAPA) to address a privacy issue for cloud storage. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications. In reduplication method prevent the unauthorized use of data accessing and create duplicate data on cloud the encryption technique to encrypt the data before stored on cloud server. In using advanced deduplication system supporting authorized duplicate check. In this new deduplication system, a hybrid cloud architecture is introduced to solve the problem.

Advantages:

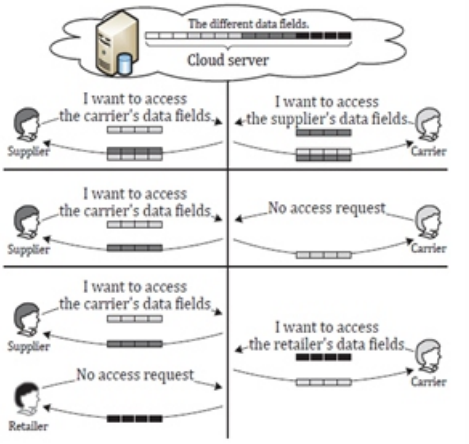
1) Shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security).

2) Attribute based access control 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 provide data sharing among the multiple users.

4) Data deduplication is one of the techniques which used to solve the repetition of data.

5) The deduplication techniques are generally used in the cloud server for reducing the space of the server.



IMPLEMENTATION:

Owner Registration: In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

Owner Login: In this module, any of the above mentioned person have to login, they should login by giving their emailid and password .

User Registration: In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

User Login: If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

Access Control: Owner can permit access or deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Encryption & Decryption: Here we are using this aes_encrypt & aes_decrypt for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt it.

File Upload: In this module Owner uploads the file(along with meta data) into database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it.

File Download: The Authorized users can download the file from cloud database.

Cloud Service Provider Registration: In this module , if a cloud service provider(maintainer of cloud) wants to do some cloud offer , they should register first.

Cloud Service Provider Login: After Cloud provider gets logged in, He/ She can see Cloud provider can view the files uploaded by their clients. Also upload this file into separate Cloud Database

TTP (TRUSTED THIRD PARTY) LOGIN: In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .Also ttp checks the CSP(CLOUD SERVICE PROVIDER),and find out whether the csp is authorized one or not.

CONCLUSION:

In this work, a new privacy challenge has been identified during accessing of data in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is implanted to guarantee data confidentiality and data integrity. Since the wrapped values are exchanged during transmission ,data anonymity is achieved. User privacy is increased by anonymous access requests to inform the cloud server in private about the users' access needs.

Forward security is accomplished by the session identifiers to stop the session correlation. It shows that the proposed scheme is perhaps applied for increasing privacy preservation in cloud applications. Data anonymity is achieved since the wrapped values are exchanged during transmission.

User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

FUTURE WORK:

In this work, though we have identified and studied a new privacy challenge in the cloud computing that is achieving privacy-preserving access authority sharing, the actual implementation of the trusted third party and then monitoring the performance will be the future scope. The actual calculations and the observations should be made to make sure the performance is not decreased but improved.

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 Multicloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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 Multi-Owner 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, and A. Nayak, "Decentralized Access Control 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.

[20] R. S´anchez, F. Almenares, P. Arias, D. D´ıaz-S´anchez, and A. Mar´ın, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing," IEEE Transactions on Consumer Electronics, vol. 58, no. 1, pp. 95-103, 2012.

[21] H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 9, pp. 1432-1437, 2011.

[22] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," in Proceedings of Global Telecommunications Conference (GLOBECOM 2010), December 6-10, 2010.

[23] I. T. Lien, Y. H. Lin, J. R. Shieh, and J. L. Wu, "A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-nn Search," IEEE Transactions on Information Forensics and Security, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6476681, 2013.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[24] A. Barsoum and A. Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6392165, 2013.

[25] H. Y. Lin and W. G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, 2012.

[26] J. Yu, P. Lu, G. Xue, and M. Li, "Towards Secure Multi- Keyword Top-k Retrieval over Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6425381, 2013.

[27] K. W. Park, J. Han, J. W. Chung, and K. H. Park, "THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment,"IEEE Transactions on Services Computing, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6133267, 2012.

[28] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," in Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS 2001), pp. 136-145, October 14-17, 2001.

[29] Helion IP Core Products: Data Security Products [Online]. Available: http://www.heliontech.com/core.htm

Author Details:

Author 1:

Kukati.Siva Prasad Was Born In Gudur [T] [M], S.P.S.R.Nellore [Dt], Andhra Pradesh, India. He Received The B.Tech Degree In Computer Science & Engineering From Jnt University, Anantapur In 2010 And Pursuing M.Tech Degree In Software Engineering From Jnt University, Anantapur. He Completed His B.Tech Degree In Audisankara College Of Enigineering & Technology, Gudur [T] [M], S.P.S.R.Nellore [Dt], Andhra Pradesh And M.Tech Degree In Skr College Of Engineering & Technology, Konduru Satram [V], Manubolu [M], S.P.S.R.Nellore [Dt], Andhra Pradesh, India.

Author 2:

Mr. Syed Baji Was Born In Andhra Pradesh, India. He Received The Bachelor Of Computer Applications Degree From Sri Krishnadevaraya University, Anantapur In 1998-2001 And Master Of Science In Information Technology From Bharath Institute Of Science & Technology, Madras University, Chennai In 2001-2003 And Master Of Technology In Information Technology From Bharath Institute Of Higher Education & Research From Bharath University, Chennai In 2003-2005. He Has 10 Years Experience In The Field Of Associate Professor And Hod In Dept .Of Cse & It. He Had Working As Associate Professor And P.G Co-Ordinator In Dept. Of Software Engineering In Skr College Of Engineering & Technology, Konduru Satram [V], Manubolu [M], S.P.S.R Nellore [Dt], Andhra Pradesh, India.