ISSN:2320-0790

An International Journal of Advanced Computer Technology

Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing

[1]Mr.Ar.Arunachalam, [2]Deepak Kumar, [3]Atul Ranjan

[1]Assistant Professor, [2,3]Undergraduate Student
Department of Computer Science,
Bharath univesity, Chennai

Abstract: Cloud services give nice conveniences for the users to get pleasure from the on-demand cloud applications while not considering the native infrastructure limitations. Throughout the information accessing, completely different users is also in a very cooperative relationship, and so knowledge sharing becomes vital to attain productive edges. the prevailing security solutions principally concentrate on the authentication to understand that a user's privative knowledge can\'t be unauthorized accessed, however neglect a delicate privacy issue throughout a user difficult the cloud server to request alternative users for knowledge sharing. The challenged access request itself could reveal the user's privacy regardless of whether or not or not it will acquire the information access permissions. Many schemes using attribute-based cryptography (ABE) are projected for access management of outsourced knowledge in cloud computing.

Key words- Attribute based cryptography(ABE), reveal

I. 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.

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.

II. RELATED WORK

Paper [1] proposes to we have a tendency to gift 2 absolutely secure practical cryptography schemes. Our test results a completely secure attribute-based cryptography (ABE) theme. Previous constructions of ABE were solely established to be by selection secure.

Paper [2] proposes to a cipher text policy attribute primarily based coding system, a user's personal key\'s related to a group of attributes (describing the user) and an encrypted cipher text can specify an access policy over attributes.

Paper [3] we gift a brand new methodology for realizing Cipher text-Policy Attribute secret writing (CP-ABE) underneath concrete and no interactive science assumptions within the customary model. Our solutions permit any encrypted to specify access management in terms of any access formula over the attributes within the system.

Paper [4] we develop a brand new methodology for utilizing the previous techniques to prove selective security for useful cryptography systems as a right away ingredient in fashioning proofs of full security. This deepens the link between the selective and full security models.

Paper [5] proposes to Cloud computing may be a revolutionary computing paradigm that permits versatile, on-demand and affordable usage of computing resources. Those benefits, ironically, square measure the causes of security and privacy issues, that emerge as a result of the information closely-held by totally different users .

Paper [6] proposes propose a Multi-Authority Attribute-Based cryptography (ABE) system. In our system,any party will become AN authority and there\'s no demand for any world coordination other than the creation of AN initial set of common reference parameters..

Paper [7] proposes a Ciphertext-Policy Attribute primarily based encoding (CP-ABE) is a promising cryptologic primitive for fine-grained access control of shared information. In CP-ABE, every user is associated with a group of attributes

Paper [8] proposes a completely useful identity-based cryptography theme (IBE). The theme has chosencip hertext security within the random oracle model forward a variant of the procedure DiffieHellman problem.

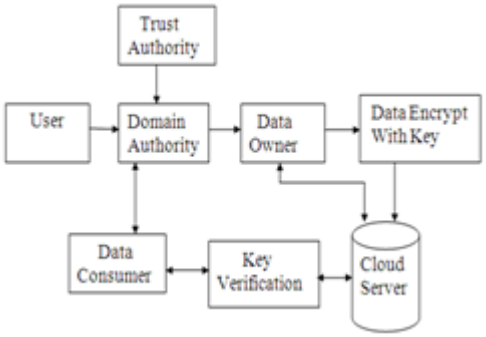
Paper [9] proposes to Personal health record (PHR) is associate degree rising patient-centric model of health info exchange, that is commonly outsourced to be hold on at a 3rd function, like cloud providers.

Paper [10] proposes A promising approach to mitigate the privacy risks in on-line Social Networks (OSNs) is to shift access management social control from the OSN supplier to the user by suggests that of encoding.

III. SECURED DATACOMMUNICATION IN CLOUD COUMPUING

A shared authority primarily based privacy-preserving authentication protocol (SAPA) to handle on top of privacy issue for cloud storage. Within the SAPA, shared access authority is achieved by anonymous access request matching mechanism with -*security and privacy concerns (e.g., authentication, knowledge obscurity, user privacy, and forward security attribute). Despite the tremendous advantages, outsourcing computation to the industrial public cloud is additionally depriving customers' direct management over the systems that consume and turn out their information throughout the computation, that inevitably brings in new security considerations and challenges towards this promising computing model. The user will solely access its own knowledge fields proxy re-encryption is applied by the cloud server to supply knowledge sharing among the multiple users.

IV. ARCHITECTURE AND MODULES DETAILS



4.1 Data Owner:

Data Owner will use the command to cipher a file to form a replacement encrypted file. The time for this operation depends on the access tree structure. in keeping with the amount of leaf nodes and also the level of the access tree policy, the time needed to cipher the file knowledge house owners and also the service suppliers area unit at intervals identical trusty domain.

4.2 Data Consumer:

The cloud automatic data processing system into consideration consists of 5 forms of parties: a cloud service supplier, information homeowners, information shoppers, variety of domain Authorities, and a trusty authority. The cloud service supplier manages a cloud to produce information storage service. Information homeowners write their information files and store.Them within the cloud for sharing with information shoppers.

4.3 Domain level Security:

The trustworthy authority is that the root authority and answerable for managing superior domain authorities. every superior domain authority corresponds to a superior organization, like a federate enterprise, whereas every lower-level domain authority corresponds to a lower-level organization, like associate degree related Company in an exceedingly federate enterprise. Knowledge owners/consumers might correspond to staff in a company. **Attribute based security:**

A data specifies an access structure for a costless text that is named because the cipher text policy. Solely users with secret writing keys whose associated attributes, laid out in their key structures, satisfy the access structure will rewrite the cipher text. Key Structure: we tend to use a algorithmic set primarily based key structure as in wherever every component of the set is either a group or a component akin to AN attribute. For a key structure with depth two, members of the set at depth one will either be attribute components or sets however members of a group at depth two might solely be attribute components.

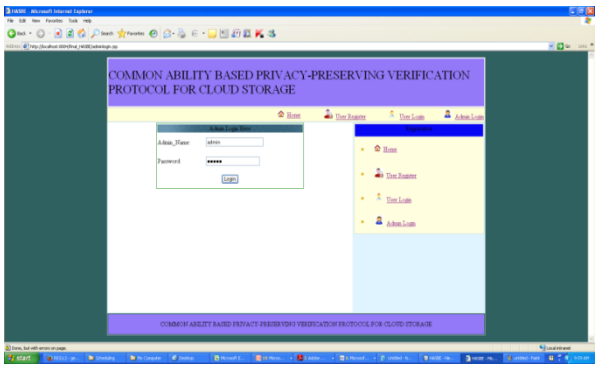
4.4 Secret files accessing:

To access the shared info files, info customers transfer encrypted information files of their interest from the cloud so decipher them. every information owner/consumer is administrated by a website authority. Within the data structure of the system users given in every party is related to a public key and a personal key, with the latter being unbroken on the Q.T. by the party. The trusty authority acts because the root of trust and authorizes the ranking domain authorities.

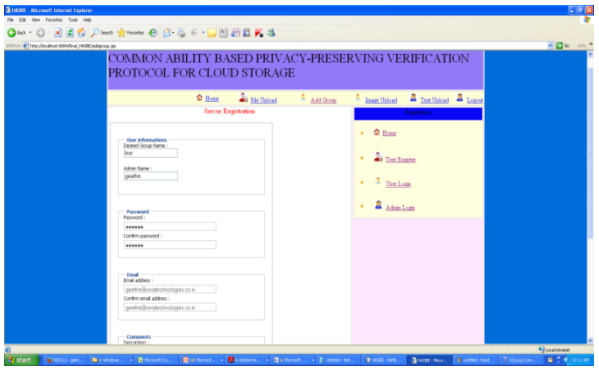
SCREEN SHOTS

HOME PAGE

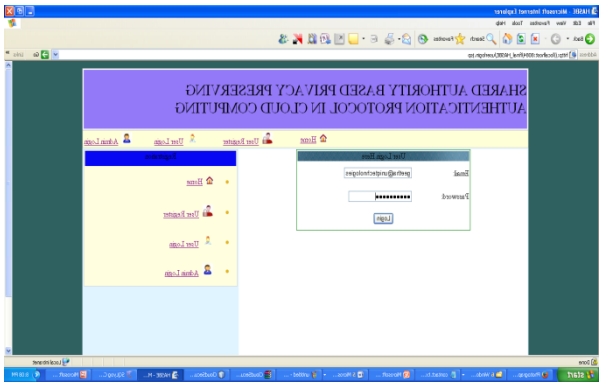
LOGIN PAGE



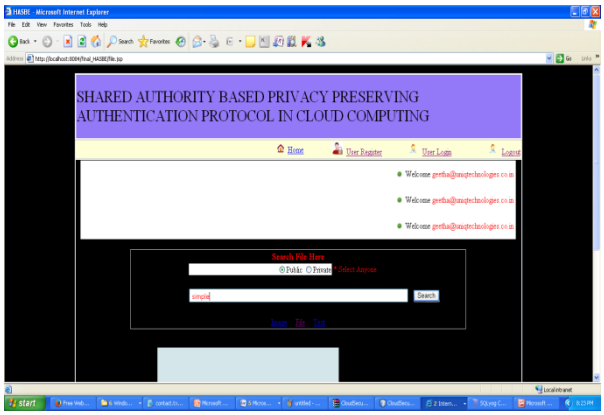
SERVER REGISTATION



LOGIN PAGE



SERCH FILE



VI. EXPERIMENTAL SETUP

Software requirement of this project includes as front end as html, java while hardware requirements include windows OS, RAM 512 MB, Pentium-III processor and HDD 20GB. In this paper we upload file, text and images where user can upload the file via two mode public and private in that public user don't have to need any type of secrete key they can download without any key and in private mode using secrete key that secrete key will be generate in give email and user will be enter the key and they can be upload the file

V. CONCLUSIONS

In this paper, we have a tendency to introduced the HASBE theme for realizing scalable, flexible, and fine-grained access management in cloud computing. The HASBE theme seamlessly incorporates a data structure of system users by applying a delegation formula to ASBE. HASBE not solely supports compound attributes as a result of versatile attribute set mixtures, however conjointly achieves economical user revocation thanks to multiple worth assignments. We formally well-tried the protection of HASBE supported the protection of CP-ABE by Bettencourt et al.. Finally, we have a tendency to enforce the projected theme, and conducted comprehensive performance analysis and analysis, that showed its potency and benefits over existing schemes.

ACKNOWLEDGMENT

THIS WORK WAS SUPPORTED BY OUR FACULTIES AT BHARATH UNIVERSTY.

REFERENCES

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

[2] 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.

[3] 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 ConsumerElectronics, vol. 58, no. 1, pp. 95-103, 2012.

[4] 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.

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

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

[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] 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.

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