IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 2, 2015, Page.848-853, ISSN: 2347–8586

Anonymous Access Control by SAPA in Cloud Computing

A.Gomathi[1] P.Mohanavalli[2]

[1]PG Student [2]Assistant Professor
[1&2]Dept. of Computer Science and Engineering
Idhaya Engineering College for Women
gomathiarul1990@gmail.com

Abstract:

Cloud computing is rising as a prevailing information interactive paradigm to understand users' information remotely hold on in a web cloud server. The present security solutions in the main specialize in the authentication to understand that a user's privative information can not be unauthorized accessed, however neglect a delicate privacy issue throughout a user difficult the cloud server to request alternative users for information 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. In this paper, we tend to propose a shared authority primarily based privacy-preserving authentication protocol (SAPA) to deal with higher than privacy issue for cloud storage. within the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy issues (e.g., authentication, information obscurity, user privacy, and forward security); 2) attribute primarily based access management is adopted to understand that the user will solely access its own information fields; 3) proxy re-encryption is applied by the cloud server to produce information sharing among the multiple users. Meanwhile, universal composability (UC) model is engaging for multi-user cooperative cloud applications.

Index Terms*—Cloud computing, authentication protocol, privacy preservation, shared authority, universal compos ability.*

1. INTRODUCTION

Cloud computing could be a promising info technology design for each enterprises and people .It launches a pretty information storage and interactive paradigm with obvious blessings, together with on-demand self-services, omnipresent network access ,and location freelance resource pooling . Towards the cloud computing, a typical service design is something as a service (XaaS), within which infrastructures, platform, software, et al square measure applied for omnipresent interconnections. Recent studies are worked to market the cloud computing evolve towards the net of services . later, security and privacy problems are getting key considerations with the increasing quality of cloud services .Conventional security approaches primarily concentrate on the sturdy authentication to appreciate that a user will remotely access its own information in on-demand mode alongside the range of the applying necessities ,users might want to access and share every other's licensed information fields to realize productive edges, that brings new security and privacy challenges for the cloud storage.

For the final case, once the shopper stores his information on multi-cloud servers, the distributed storage and integrity checking square measure indispensable. On the opposite hand, the integrity checking protocol should be economical so as to create it appropriate for capacity-limited finish devices. Thus, supported distributed computation, we'll study distributed remote information integrity checking model and gift the corresponding concrete protocol in multi-cloud storage.

In the cloud environments, an affordable security protocol should attain the subsequent needs.

1) **Authentication:** a legal user will access its own information fields, only the approved partial or entire information fields are often identified by the legal user, and any cast or tampered data fields cannot deceive the legal user.

2) **Information anonymity:** any extraneous entity cannot acknowledge the changed data and communication state even it intercepts the exchanged messages via Associate in Nursing open channel.

3) **User privacy:** any extraneous entity cannot apprehend or guess a user's access desire, that represents a user's interest in another user's approved information fields. If and providing the each users have mutual interests in every other's approved data fields, the cloud server can inform the to users to realize the access permission sharing.

4) **Forward security:** any someone cannot correlate to communication sessions to derive the previous interrogations in keeping with the presently captured messages.In this work, tendency is to aim to handle a user's sensitive access need connected privacy throughout information sharing within the cloud environments, and it's important to design a

humanistic security theme to at the same time achieve information access management, access authority sharing, and privacy preservation.

2. SYSTEM WORK

Hong liu et al [1] address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are as follows. 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. Dunning *et al.* [2] proposed associate anonymous ID assignment based information sharing algorithmic rule (AIDA) for multiparty oriented cloud and distributed computing systems. In the AIDA, associate number information sharing algorithmic rule is intended on high of secure add data processing operation, and adopts a variable and infinite range of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem square measure used for the information mining, a distributed answer of sure polynomials over finite fields enhances the algorithmic rule quantifiability, and Markov chain representations square measure accustomed confirm statistics on the required range of iterations.

Liu et al. [3] projected a multi-owner information sharing secure theme (Mona) for dynamic teams within the cloud applications. The Anglesea aims to understand that a user will securely share its information with alternative users via the untrusted cloud server, and may with efficiency support dynamic cluster interactions. within the theme, a brand new granted user will directly decrypt information files while not pre-contacting with information while not change the key keys of the achieved by a remaining users. Access management is applied to confirm that any user in a cluster will anonymously utilize the cloud resources. The information owners' real identities will solely be unconcealed by the cluster manager for dispute arbitration. It indicates the storage overhead and cryptography computation price are freelance with the number of the users.

Grzonkowski et al. [4] planned a zero-knowledge proof (ZKP) based mostly authentication theme for sharing cloud services. supported the social home networks, a user centrical approach is applied to modify the sharing of customized content and complex network-based services via TCP/IP infrastructures, during which a trusty third party is introduced for suburbanized interactions. Nabeel et al. [5] planned a broadcast cluster key management (BGKM) to boost the weakness of radially symmetrical key cryptosystem publicly clouds, and therefore the BGKM realizes that a user needn't utilize public key cryptography, and can dynamically derive the radially symmetrical keys throughout decryption. consequently, attribute based mostly access management mechanism is intended to realize that a user will decipher the contents if and on condition that its identity attributes satisfy the content provider's policies. The fine-grained formula applies access management vector (ACV) for distribution secrets to users supported the identity attributes, and allowing the users to derive actual radially symmetrical keys based mostly on their secrets and different public info. The BGKM has a lucid advantage throughout adding/revoking users and change access management policies.

Wang et al. [6] planned a distributed storage integrity auditing mechanism, that introduces the homomorphic token and distributed erasure-coded knowledge To enhance secure and dependable storage services in cloud computing. The theme permits users to audit the cloudstorage with light-weight communication overloads and computation price, and therefore the auditing result ensures sturdy cloud storage correctness and quick knowledge error localization.Towards the dynamic cloud knowledge, the theme supports dynamic outsourced knowledge operations. It indicates that the scheme is resilient against Byzantine failure, malicious data modification attack, and server colluding attacks.

Sundareswaran et al. [7] established a decentralized information responsibleness framework to trace the users' actual knowledge usage within the cloud, and planned an object-centered approach to alter intromission the work mechanism with the users' knowledge and policies. The Java ARchives (JAR) programmable capability is leveraged to create a dynamic and mobile object, and to confirm that the users' knowledge access can launch authentication ,in addition ,distributed auditing mechanisms also are provided to strengthen user's knowledge management, and experiments demonstrate the approach potency and effectiveness. In the said works, varied security problems are addressed . However, a user's refined access request related privacy drawback caused by knowledge accessing and data sharing has not been studied nonetheless within the literature. Here, tendency is to determine a replacement privacy challenge, and propose a protocol not solely specializing in authentication to realize the valid knowledge accessing, however conjointly considering authorization to produce the privacy-preserving access authority sharing. The attribute based mostly access management and proxy re-encryption mechanisms are collectively applied for authentication and authorization.

3. PROBLEM STATEMENT

In the cloud storage based supply chain management, there are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier purposely may want to access a carrier's data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations.

4. SYSTEM MODEL

In the cloud storage, a user remotely stores its knowledge via online infrastructures, flat forms, or computer code for cloud services, that are operated within the distributed, parallel, and cooperative modes. Throughout cloud knowledge accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and freelance authority on its own knowledge fields. It is necessary to ensure that the users' outsourced knowledge cannot be unauthorized accessed by alternative users, and is of essential importance to confirm the non-public info during the users' knowledge access challenges. In some situations ,there are multiple users in a very system (e.g., supply chain management), and also the users may have totally different affiliation attributes from totally different interest teams. One of the users might want to access alternative associate users data fields to attain bi-directional knowledge sharing, but it cares concerning two aspects: whether or not the aimed user would like to share its knowledge fields, and the way cannot expose its access request if the aimed user declines or ignores its challenge. within the paper, I have a tendency to pay a lot of attention on the process of knowledge access management and access authority sharing aside from the precise file directed cloud knowledge transmission and management.

4.1 OWNER

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, any of the above mentioned person have to login, they should login by giving their email id and password. Owner must give permission to download or to access the owner private data .if they permitted means user access the owners data.

4.2 USER

An individual or cluster entity, which owns its information hold on within the cloud for on-line information storage and computing. totally different users could also be related to with a typical organization, and square measure allotted with independent authorities on bound information fields .Being rational means that Users behavior would be never based on experience or emotion, and misbehavior may only occur for selfish interests.

4.3 CLOUD SERVER

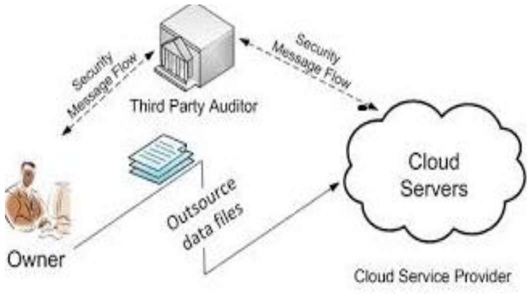

FIG 3.1 CLOUD SERVER MODEL

Associate entity, that is managed by a selected cloud service supplier or cloud application operator to produce information storage and computing services. The cloud server is thought to be associate entity with unrestricted storage and process resources. fig 3.1 shows the cloud server model in that owners outsource their data files into the cloud server.

4.4 CLOUD SERVER ACCESS CONTROL

Being semi-honest means that cloud server can be regarded as an entity that appropriately follows the protocol procedure. Being curious means that cloud server may attempt to obtain users private information (e.g., data content, and user preferences). It means that cloud server is under the upervision of its cloud provider or operator, but may be interested in viewing users' privacy.In the passive or honest but-curious model, cannot tamper with the users' data to maintain the system normal operation with undetected monitoring.

4.5 ENCRYPION AND DECRYPION

AES used for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt using AES. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data? the data to be encrypted. This array we call the state array.

The following steps to encrypt a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data.
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data.

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D_0 / D_{15}, are loaded into the array. Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- Substitute Bytes
- Shift Rows
- Mixed Columns
- Add Round Key

4.6 TRUSTED HIRD PARTY

Associate optional and neutral entity, which has advanced capabilities on behalf of the users, to perform information public auditing and dispute arbitration. Towards the threat model, it covers the possible security threats and system vulnerabilities during cloud data interactions. The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content.

5. SYSTEM ARCHITECTURE

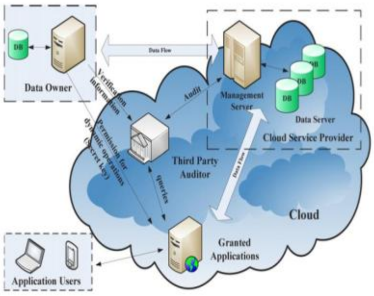

FIG 3.1 SYSTEM ARCHITECTURE

6. SAPA PROTOCOL

To address the same privacy issue to propose a shared authority based mostly privacy preserving authentication protocol (SAPA) for the cloud data storage, that realizes authentication and authorization without compromising a user's personal data. The main contributions area unit as follows;

1) determine a replacement privacy challenge in cloud storage, and address a delicate privacy issue throughout a user challenging the cloud server for information sharing, in which the challenged request itself cannot reveal the user's privacy regardless of whether or not or not it will obtain the access authority.
2) Propose associate degree authentication protocol to boost a user's access request connected privacy, and also the shared access authority is achieved by anonymous access request matching mechanism.
3) Apply cipher text-policy attribute based mostly access management to realize that a user will faithfully access its own information fields, and adopt the proxy re-encryption to provide worker approved information sharing among multiple users.

7.SEURIY MODEL

7.1 Universal Composability Model

Universal compos ability (UC) model is established to prove that the SAPA 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.

The universal composability (UC) model specifies an approach for security proofs , and guarantees that the proofs will remain valid if the protocol is modularly composed with other protocols, and/or under arbitrary concurrent protocol executions. There is a real-world simulation, an ideal-world simulation, and a simulator translating the protocol execution from the real world to the ideal-world. Additionally, the Byzantine attack model is adopted for security analysis, and all the parties are modeled as probabilistic polynomial-time Turing machines (PPTs), and a PPT captures whatever is external to the protocol executions. The adversary controls message deliveries in all communication channels, and may perform malicious attacks (e.g., eavesdropping, forgery, and replay), and may also initiate new communications to interact with the legal parties.

7.2 PRIVATE MATCHING

Private matching (PM) is a value matching protocol. It assists two interactive entities to compute set intersection over their private set of values, without revealing any element of their private set to each other. It uses homomorphic encryption to identify the commonalities among the private sets, while ensuring privacy of each set. Suppose there is a client *C* and a server *S*. *C* has its own private set of values $X : \{x1, x2 \ldots xn\}$, and so does *S*, $Y : \{y1, y2 \ldots yn\}$. *C* wants to compute set intersection with *S* over the private set of values (i.e. *X*,*Y*). However, *C* does not want to seep out any information about *X*, with an exception of set cardinality.

8. CONCLUSION

The replacement privacy challenge during information accessing within the cloud computing to realize privacy-preserving access authority sharing. Authentication is established to ensure information. confidentiality and information integrity, information obscurity is achieved since the wrapped values area unit changed throughout transmission. User privacy is increased by anonymous access requests to in camera inform the cloud server concerning the users' access wishes. Forward security is accomplished by the session identifiers to stop the session correlation. It indicates that the projected theme is probably applied for increased privacy preservation in cloud applications.

REFERENCES

[1] Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong , Member, *IEEE* ,and Laurence T. Yang,, Member, *IEEE* "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing" 2014.

[2] 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.

[3] 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, 2013.

[4] 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, 2012.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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=6463404,2011.