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

Information Sharing Used To Security Protocols in Cloud Computing

Bosubabu Sambana
MCA, M.Tech (CSE),
Assistant Professor, Department of Computer Science & Engineering,
Simhadri Engineering College, Visakhapatnam, AP-531001, India.

Abstract:

Cloud services provide great user friendly and conveniences for the users/clients to easy the on-demand base cloud applications without considering the local infrastructure limitations. It's works on client-server architecture model. Client sends to message packet server receive and send acknowledgement in their response, after active to send what they need user need in sorting manner. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. 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 reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose a SAPA and other Security protocols and using AES algorithm to address above 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 computing applications.

Index Terms :

Cloud computing; cloud Storage, authentication protocol, Security Protocols, privacy preservation, shared authority, universal composability AES algorithm.

1. INTRODUCTION:

Cloud computing is a promising information technology architecture for both enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self-services, ubiquitous network access, and location independent resource pooling [1].

Towards the cloud computing, typical service architecture is anything as a service (XaaS), in which infrastructures, platform, software, and others are applied for ubiquitous interconnections. Recent studies have been worked to promote the cloud computing evolve towards the internet of services [2], [3]. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of cloud services. Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage.

2. BACKGROUND

2.1 Cloud computing:

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..

2.2.Authentication:

A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

2.3.Cloud Characteristic:

One of the oft-cited advantages of cloud computing is its elasticity in the face of changing conditions.

For example, during seasonal or unexpected spikes in demand for a product retailed by an e-commerce company, or during an exponential growth phase for a social networking Website, additional computational resources can be allocated on the fly to handle the increased demand in mere minutes. Similarly, in this environment, one only pays for what one needs, so increased resources can be obtained to handle spikes in load and then released once the spike has subsided. Having DBMS in the cloud will give advantage in fast and elastic computing.

2.4.Cloud storage:

Cloud storage means the storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

2.5.Data anonymity :

Any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.

2.6. Forward security :

Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

2.7 User/Client privacy :

Any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

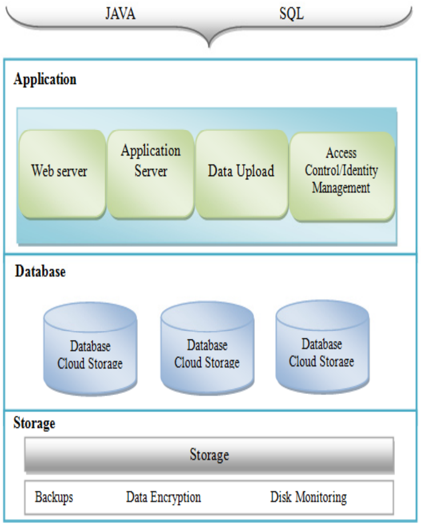


Fig. 1. DBMS in the Cloud Architecture

3.RELATEDWORK:

Wang et al. [4] proposed a distributed storage integrity auditing mechanism, which introduces the homomorphism token and distributed erasure-coded data to enhance secure and dependable storage services in cloud computing. The scheme allows users to audit the cloud storage with lightweight communication overloads and computation cost, and the auditing result ensures strong cloud storage correctness and fast data error localization. Towards the dynamic cloud data, the scheme supports dynamic outsourced data operations. It indicates that the scheme is resilient against Byzantine failure, malicious data modification attack, and server colluding attacks.

Sundareswaran et al. [5] established a decentralized Information accountability framework to track the users' actual data usage in the cloud, and proposed an object-centered approach to enable enclosing the logging mechanism with the users' data and policies. The Java ARchives (JAR) programmable capability is leveraged to create a dynamic and mobile object, and to ensure that the users' data access will launch authentication. Additionally, distributed auditing mechanisms are also provided to strengthen user's data control, and experiments demonstrate the approach efficiency and effectiveness.

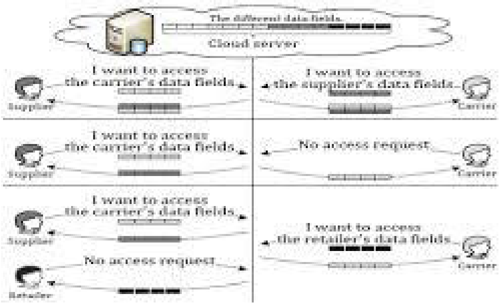

The different data fields
Cloud server
I want to access the carrier's data fields
I want to access the supplier's data fields
Supplier
Carrier
I want to access the carrier's data fields
No access request
Supplier
Carrier
I want to access the carrier's data fields
I want to access the retailer's data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

Fig.2. Three possible cases during data accessing and data sharing in cloud applications.

3.1.The Shared Authority Based Privacy Preserving Authentication Protocol

The SAPA adopts integrative approaches to address ecure authority sharing in cloud applications.

System Framework:

In this paper, we address the above-mentioned privacy issue to propose privacy preserving authentication protocol (SAPA) for the cloud data storage, based on cloud storage which gives authentication and authorization without conceding a user's private information. The main consideration will be as follows:

1) A new privacy challenge in cloud storage is to be located and also to identify an indirect privacy for data sharing, in which the challenged request itself cannot get the user's privacy
2) Design an authentication protocol which enhances a user's access request, which is related to the privacy. The shared access authority is achieved by unidentified access request matching mechanism.
3) Cipher text-policy is applied and a user can access its own data fields and proxy re-encryption is accepted to provide authorized data sharing among multiple users [6].

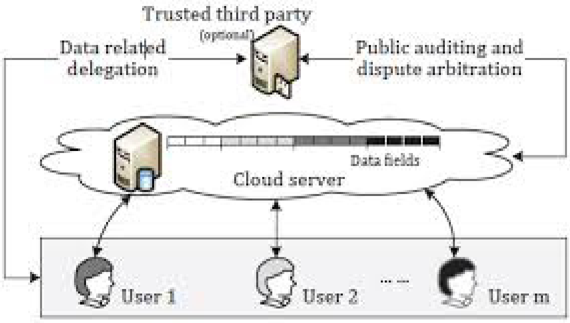


Fig. 3. The cloud storage system model.

Use of AES Algorithm:

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, nonlinearity of the key expansion practically eliminates the possibility of equivalent keys in AES.Amongst AES, DES and Triple DES for different microcontroller's comparison is made then it shows that AES has a computer cost of the same order as required for Triple DES [7].

Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blowfish in terms of time consumption.

4. REASEARCH WORK:

Existing System:

However, most previous researches focus on the authentication to realize that only a legal user can access its authorized data, which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits. When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation.

Disadvantage:

Previous System does not have the option of granting / revoking data access.

Proposed System:

In this paper, we 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.

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.

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

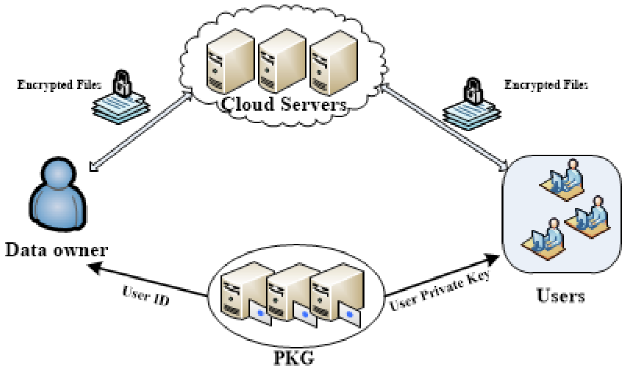
Advantage:

Here we proposed the secured system and data owner can decide whether the user can access the system or not.

PROBLEM STATEMENT :

In our model, privacy is accomplished by encrypting the data it can prevent the un authorized access. Scope: We are going to raise the privacy level of the data owner and the confidentiality of the data by providing access to users.

Architecture:



Modules :

1. Owner
2. User
3. Access Control
4. Cloud Service Provider (CSP)
5. Cryptography- Encryption & Decryption
6. File Download
7. Trusted Third Party

In Detailed Modules Description

Owner Registration: In 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 owner login session, any one of the above mentioned user/person have to login, they should login by giving their email-id and password. If Owner Provides more security mechanism.

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. Example:- Username / Password using specific authentication.

Access Control: If 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. Sometimes Hackers may be logged this files.

Cryptography - Encryption & Decryption : Here using DataEncryptionStandards (DES) and 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. Plaintext is converted into Cipher text and using files in data is 64-bit /128-bits

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 (along with meta data) from cloud database or remote system.

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 using shared files.

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 it's checks the CSP(CLOUD SERVICE PROVIDER is verified), and find out whether the CSP is authorized one or not. Unauthorized person are manage their owner/user

Account (A/c) login. if owner(Server) provides less security mechanism.

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 n company strength. Once these things r satisfied, ten next steps are 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. Before building the system the above consideration are taken into account for developing the proposed system.

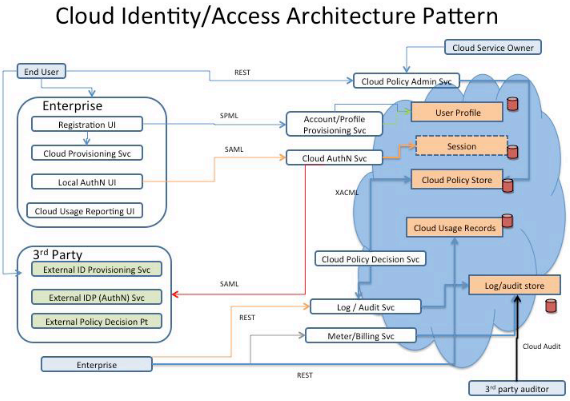


Fig .5.Cloud Servers on Permission Access

IMPLEMENTATION:

We have implemented our basic approach on Amazon S3 which is a popular cloud based storage service. The content management consists of two tasks. First, the Owner encrypts the data item sets based on the access control policies and uploads the encrypted sets along with some meta-data. Then, authorized users download the encrypted data items sets and meta-data from the Cloud, and decrypt the data item sets using the secrets they have. Now we illustrate the interactions of the Owner with Amazon S3 as the Cloud. In our implementation, we have used the REST API to communicate with Amazon S3. Figure - 6 shows the overall involvement of the Owner in the user and content management process when uploading the data item sets to Amazon S3.While the fine-grained access control is enforced by encrypting using the keys generated through the AB-GKM scheme, it is important to limit the access to even the encrypted data item sets in order to minimize the bandwidth utilization. We associate a hash-based message authentication code (HMAC) with each encrypted data item sets such that only the users having valid identity attributes can produce matching HMACs.Initially the Owner creates a bucket , which is a logical container in S3, to store encrypted data item sets as objects . Subsequently, the Owner executes the following steps:1. The Owner generates the symmetric keys using the AB-GKM's KeyGen algorithm and instantiates an encryption client. Note that the Owner generates a unique symmetric key for each policy configuration.

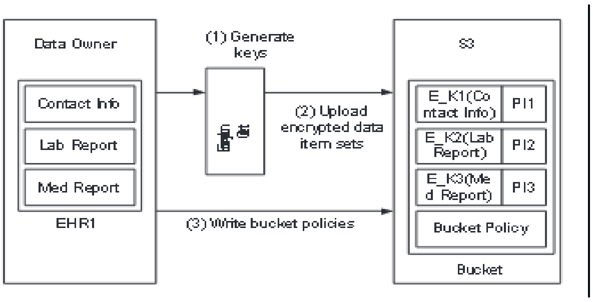


Fig..6. Implementation details

Comparison & Approaches:

In this section we compare ABE-based existing approaches as a whole and the two AB-GKM based approaches presented earlier. A common characteristic of all these approaches is that they support secure attribute based group communication.

Table 1: Comparison of Approaches

Property	ABE	SLE	TLE
Cryptography	Asymmetric	Symmetric	Symmetric
Secure attribute based group Communication	Yes	Yes	Yes
Delegation of Access Control	No	No	Yes
Efficient revocation	No	Yes	Yes

As shown in Table-1,while ABE-based approaches rely on asymmetric cryptography, our two approaches rely only on symmetric cryptography which is more efficient than the asymmetric cryptography. A key issue in the ABE-based approaches is that they do not support efficient user revocations unless they use additional attributes [8]. Our schemes address the revocation issue. It should be noted that the ABE based approaches and our SLE approach follows the conventional data outsourcing scenario by which the data owner manages all users and data before uploading the encrypted data to the cloud, whereas the TLE based approach provides the advantage of partial management of users and data in the cloud itself while assuring confidentiality of the data and privacy of users.

With ever increasing user base and large amount of data, while such delegation of user management and access control is becoming very important, it also has trade offs in terms of privacy. Compared to the SLE approach, in the TLE approach, the data owner has to reveal partial access control policies to the cloud which may allow the cloud to infer some details about the identity attributes of users. It is an interesting topic to investigate how to construct symmetric key based practical solutions to hide the access control policies from the cloud while utilizing the benefits of delegation of control.

5. CONCLUSION:

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. 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.

ACKNOWLEDGMENT:

This paper is Heartily Dedicated to my beloved Parents Sri.S.Dandasi & Smt.Janaki and My life Inspirer Eminent Scientist Sri.Dr.A.P.J.Adbulkalam.

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.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,", [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, 2012.

[4]C. Wang, Q. Wang, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions onServices Computing, vol. 5, no. 2, pp. 220-232, 2012.

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

[6]Hong Lui, Huansheng ,Qingxu Xiong," Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transaction, vol. pp no. 99, 2014.

[7]Midya AzadIsmail, KlinsegaJeberson,"Secure Data Sharing Through Cloud Computing", In International Journal of Computer Engineering & Technology(IJCET), 2014,vol. 5,pp. 41-47

[8] J. Camenisch, M. Dubovitskaya, R. R. Enderlein, and G. Neven.Oblivious transfer with hidden access control from attribute-based encryption. In SCN 2012: Proceedings of the 8th International Conference on Security and Cryptography for Networks, pages 559–579, 2012.

[9]All Images and Related information: www.google.com/

Author's Profile:

Bosubabu Sambana working with as an Assistant Professor in Simhadhri College of Engineering, Visakhapatnam.He is completed Master Degree of Computer Applications and Master Degree in Computer Science & Engineering from Jawaharlal Nehru Technological University – Kakinada , pursing Master of Science in Mathematics,Andhra University, Andhra Pradesh, India. He has 3 years good teaching experience and having a good Knowledge on Computer Science Subjects.He is Published 4 Papers in Various International Journals. He is the member of INTERNET SCOCIETY ,W3C,MECS-PRESS,IAENG,IAAE and IJECSE..