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

Privacy-preserving Authentication Protocol using Trusted Third Party Secure Data Sharing in Cloud Computing

Bosubabu Sambana, MCA, M.Tech
Assistant Professor,
Dept of Computer Science & Engineering,
Simhadhri Engineering College, Visakhapatnam, AP-531001, India.

Abstract:

Cloud computing is emerging as a prevalent data interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. 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 shared authority based 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 composability (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.

Keywords:

Cloud computing, cloud Storage, authentication protocol, privacy preservation, shared authority, universal composability.

1. INTRODUCTION:

"Cloud" is a tenure used for a simulated collection of computing means. An extensive range of benefits are accessible to consumers using cloud computing: availability of a huge collection of software applications, apparently limitless storage, access to fast treating power and the ability to easily share information across the world. A user can access all of these welfares through his or her browser any time once he/she has right of entry to the Internet. In the initial 1990s, a huge ATM network started being called to as "cloud" [1]. The term appeared once again about twelve years before with the entrance of Amazon's web-based services. Cloud computing agrees consumers and corporate structures to custom all the applications offered by the cloud deprived of the extra effort of installation and also offers access to their personal files from any computer with Internet access. Cloud computing is a complicated in terms of software, hardware and storage, all of which are

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

available as a provision. It is comprised fundamentally of applications running remotely (known as "in the cloud") which is made obtainable to all its users. The technology offers access to a large number of sophisticated supercomputers and their resultant processing power, connected at various locations around the world, thus offering lightning speed of computations [9].Cloud promises noticeable cost savings and speed to customers. Using cloud technology, a company can speedily deploy applications where expansion and contraction of the essential technology components can be accomplished with the high and low of the business life cycle.

The previous work and research shows that it can be achieved with the help of cloud enablers, such as virtualization, grid computing, that allow applications at runtime to be dynamically deployed onto the most suitable infrastructure [9]. There remain issues of reliability, privacy, security and portability even though the work may have addressed authentication. However, most investigates focused on the authentication to make sure that a user who is legally allowed to use or share, can upload its data and the major concerned is ignored that different users may tend to access and share each other's official data fields. A user realizes that the cloud server is requesting for other users for data sharing and access request itself may disclose the user's privacy.

The access to the data is may not be achieved though. This work purpose to address a user's access to the shared data and also the privacy during data sharing in the cloud surroundings, and it is significant to project a humanistic safety scheme to concurrently achieve data admission control, access authority sharing, and privacy protection.

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.

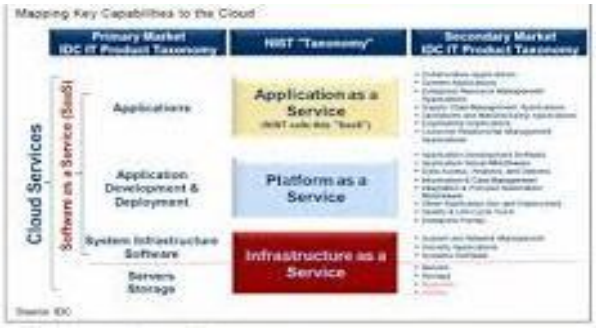


Figure.1: Cloud Computing Overview

2.2 Autantication :

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 Characteristics:

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 (instead of the many days it can take to procure the space and capital equipment needed to expand the computational resources in-house).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.

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

2.5 Data anonymicy:

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

2.6 User 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.

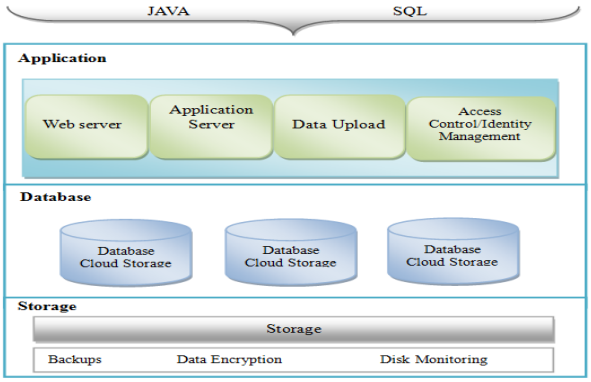


Figure.2: DBMS in the Cloud Architecture

3. RELATED WORK:

Sundareswaran et al. [12] 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.

Cloud Services:

Data privacy a lot of study has been done on the potential of cloud and the services that cloud computing can and could deal. These services can be characterized into four main sections: Storage as a Service (StaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Following section highlights these services and their usage in depth.

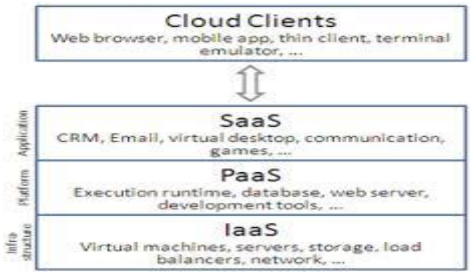


Figure.3: Cloud Server and Client process

A. Storage as a service:

Cloud offers a storage space that is huge, seemingly boundless, and rising every day. Storage as a Service (StaaS) allows cloud applications to gauge beyond their inadequate servers. Cloud storage systems needs to focus on requirements for upholding users' data and information, considering high performance, availability, replication, data reliability and reliability. The accountability to individual is maintained and upholds customer's own computer storage as cloud vendors deal them the choice of loading their information in the cloud which is reachable whenever they need [11]. Unfortunately, due to the contradictory nature of the necessities of cloud services, no one system implements all of them together.

B. Security Issues:

Companies are promptly moving onto cloud because they can now use the greatest capitals available on the market in the blink of an eye and also decrease their operations' cost radically. But as more and more information is moved to the cloud the security concerns have continuing to grow. Data breaking is the biggest security issue. A capable hacker can easily get into a client side application and get into the client's intimate data

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

[2].Incompetent and faulty APIs and interfaces become the target. IT companies which provide cloud services allow third party companies to alter the APIs and familiarize their own functionality which in turn allows these companies to comprehend the internal workings of the cloud[2].Denial of Service (DoS) is also a major menace wherein the user is approved partial or not at all access to their data. Companies now use cloud very frequently say all days and DoS can root huge increase in cost both for the user and service provider. Connection snooping is that in which a hacker can scan your online actions and copy/replay a particular broadcast to get into your private data. It can also lead to the user to unlawful or unsolicited sites. Data loss is also another issue.

A malicious hacker can wipe out the data or any natural/man-made disaster can destroy your data. In such cases having an offline copy is a big advantage. Carelessness of the service provider can also lead to data loss [3].Compatibility between different cloud services is also an issue. If a user decides to move from one cloud to another the compatibility ensures that there is no loss of data. Cloud can also be used for wrong purposes i.e. cloud abuse.Due to the availability of latest technologies on the cloud it can be used for high end calculations which cannot be done on a standard computer[2],[3].

Insufficient understanding of cloud technologies can lead to unknown levels of risk. Companies move to cloud because it provides substantial reduction in cost but if transfer is done without proper background learning, the problems that arise can be even greater. Internal intruders are able to use the data for harmful purposes. Safe storage of encryption keys is also a problem. Even if you are using encryption for enhanced security, keeping a key a safe asset becomes an issue. Who should be the owner of the key? User seems to be the answer but how diligent and careful can he/she be will decide the security of the data.

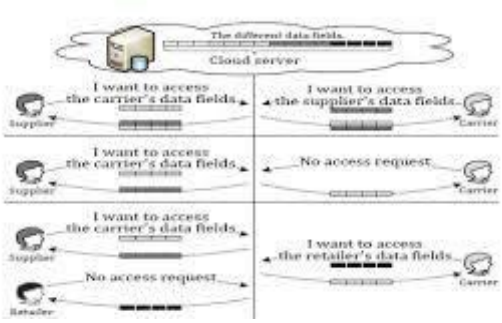


Figure.4: Three possible cases during data accessing and data sharing in cloud applications.

3.1. Privacy Preserving Authentication Protocol

This Protocol adopts integrative approaches to address secure 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].

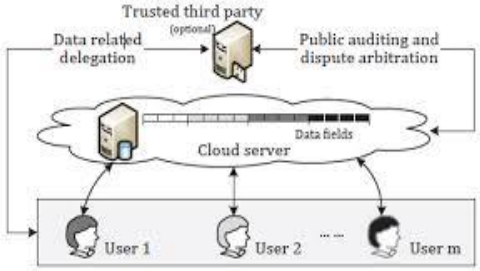


Figure.5: The cloud storage system model.

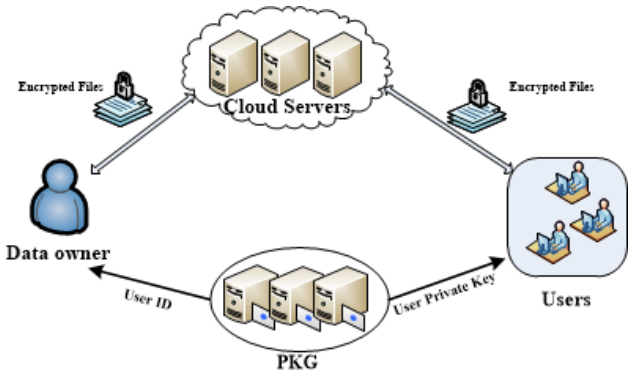
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 microcontrollers 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

System Architecture:

Following section describes the proposed system architecture with their each module description. Fig.1 shows the model of proposed system to be implemented as part of secure protocol [10].



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.

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.

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

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 Data Encryption Standards (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.

Figure. 5: Cloud services through files Transmission

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

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.

Technical Specifications Proposed:

Following technical details are considered for implementing the proposed system model. This specifies software and hardware component requirements of the system.

Software: Java 1.6/1.7 versions

Tool: Net Beans 7.1 and updated versions

Database: SQL Server 2005 / MySQL

Hardware requirements consisting of multiple user terminals, cloud environment and required computing servers.

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

Risks Analysis of Proposed Model:

RMMM plan tackles risk through Risk[13] Assessment and Risk Control. Risk Assessment involves:

a) Risk Identification,

b) Risk Analysis and

c) Risk Prioritization.

Risk Control involves Risk Resolution, Risk Management Planning and Risk Monitoring.

Purpose:

The RMMM plan outlines the risk management strategy adopted. A proactive approach is adopted to tackle risks and thus reduce the performance schedule and cost overruns, which we may incur due to occurrence of unexpected problems. This "Risk Mitigation Monitoring and Management Plan" identifies the risks associated with our project. In addition to project risk and technical risks, business risks are also identified, analyzed and documented. This document outlines the strategy that we have adopted to avoid the specified risks. A contingency plan preparation for each risk, in case it becomes a reality is maintained. Only those risks have been treated whose probability and impact are relatively high i.e. above a referent level.

Risk Table:

Impact levels:

The risks are categorized on the basis of their probability of occurrence and the impact that they would have, if they do occur. Their impact is rated as follows and shown in Table-1 for the proposed system:

a) Catastrophic - 1
b) Critical - 2
c) Marginal - 3
d) Negligible – 4

No.	Risk	Category	Probability	Impact
1	Increase of work load	Personal	20%	3

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

2	Inexperience in Project software environment	Technical	25%	3
3	Overly optimistic Schedule	Project	20%	3
4	Lack of sufficient research	Technical	50%	3
5	Module require more testing and further implementation work	Project	50%	2
6	Inconsistency in Input	Project	30%	3

Table 1. Risk Analysis of Proposed System

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 and research a new privacy challenge in the cloud computing that is achieving privacy-preserving access authority sharing process mechanism, the actual implementation of the trusted third party and then monitoring entire process of 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 hope to improved.

Acknowledgment:

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

Authors' Profiles:

Bosubabu Sambana working with as an Assistant Professor in Simhadhri Engineering College, Visakhapatnam. He is completed Master Degree in 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 4 years good teaching experience and having a good Knowledge on Space Research, Future Internet Architecture, Cloud Computing, Internet of Things/Services/Data, Computer Network and Hacking along with Computer Science Subjects. He is Published 4 Research Papers in various reputed International Journals and Magazines. He is the member of NASA, INTERNET SCOCIETY, W3C, MECS-PRESS, IAENG, IAAE and IJECSE.

REFERENCES:

[1] Rich Maggiani, 2009 Cloud Computing Is Changing How We Communicate", In IEEE 978-1-4244-4358-1/09

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

[2] The Notorious Nine, Cloud Security Alliance, February 2013[Online]Available:

http://www.cloudsecurityalliance.org/topthreats

[3] Ted Samson, Nine Top Threats to Cloud Computing Security, Info World,February 25, 2013 [Online] Available: http://www.infoworld.com

[4] Jianfeng Yang and ZhibinChen, 2010 Cloud Computing Researchand ecurity Issues",IEEE 978-1-4244-5392-4/10.

[5] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian and Aoying Zhou,2010 Security and Privacy in Cloud Computing: A Survey, In Sixth International Conference on Semantics, Knowledge and Grids. Threats in Cloud Computing, In 6th International Conference on Internet Technology and Secured Transactions.

[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Dr. Atanu Rakshit, 2009 Cloud Security Issues, In IEEE International Conference on Services Computing.

[7] Midya Azad Ismail,,"Secure Data Sharing Through Cloud Computing",(IJCET),2014,vol.5,pp.41-47

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

[9] Debajyoti Mukhopadhyay, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal, "Enhanced Security for Cloud Storage using File Encryption" Available: http://arxiv.org/ftp/arxiv/papers/1303/1303.7075.pdf

[10] 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

[11] International Journal of Engineering, Economics and Management ISSN: 2319-7927, Volume 3, Issue 1