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

Study for Enhancement in Privacy-preserving Authentication Protocol using Trusted Third Party in Cloud

Ms. Madhumita S Patil **Prof. Santosh Kumar**

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. Hence privacy criteria for an user is at risk as access request tends to expose all the information. In this paper, we have studied privacy-preserving authentication protocol (SAPA) to address the mentioned privacy issue for cloud storing and also trying to address to the efficiency increased by this SAPA protocol. It also designates that the proposed protocol realizing privacy-preserving data access authority sharing is most promising for multi-user collaborative cloud applications.**
The study and the research let us to focus on Trusted Third party mechanism. Trusted third party seems the effective measure to make sure the authentication and authorization is done with minimum interactions with cloud server.

Key Words — **Cloud Computing, Data Privacy, Security, Trusted Third Party.**

I. 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 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.

II. RELATED WORK: 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.

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 [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.

III. System Model

A. 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 [10].

In the proposed and studied framework, through file encryption securing of files is achieved. The file present on the device will be encrypted using password based AES algorithm. Any of the uploaded files which are encrypted can be downloaded by user and read it on the system. AES is not liable to be influenced by any other attack but Brute Force attack. AES is much faster than the traditional algorithms e.g. RSA. Thus, it makes a considerable choice for protection of data on the cloud [11].

It is to be noted that the proposed system works only when a stable internet connection is available. Here, the secured system and data owner can decide whether or not the user can access the system.

The efficiency check can only be confirmed after the implementation of the given proposed model. After the response timings has been measured then actual calculations will support the fact that this work has a significant value.

Use of the Trusted Third Party seems the challenging part and the most effective module. If it handles all the call from the user to access data from cloud first, it should:

1) Validate the user

2) Make sure the data for which the user is asking, authorized to that particular user.
3) If not then it should return the invalid access report to user.

In short rather than calling the cloud services or methods there should be a mediator monitoring all the authentication and authorization.

B. Use of AES Algorithm

Under a wide range of environments, AES performs consistently well in hardware and software platforms. These include 8-bit and 64-bit platforms and DSP's. Its inherent parallelism facilitates efficient use of processor resources and result in very good software performance. AES algorithm has speedy key setup time and good key agility. It requires less memory for implementation and also making it suitable for restricted-space environments. There are no serious weak keys in AES. It supports any block sizes and key sizes that are multiples of 32. The cipher text Statistical analysis has not been possible even after using huge number of test cases. No differential and linear cryptanalysis attacks have been yet proved on AES.

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 [9]. 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.

C. 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].

Owner Registration:

An owner has to upload its files in a cloud server, and then user should register first. After that only the user will be able to do it. Then Registration method is then followed. These details are stored in a database.

Owner Login:

This specifies among the registered person have to login, they should be able to login by mentioning their emailId, password.

User Registration:

If a user has to access the data from cloud, the as mentioned registration is a mandatory step to be followed and data is updated in Database.

User Login:

An authorized user can download the file by using file_id which the owner has specified already.

Access Control:

Owner can allow the access or deny access for accessing the data.

Encryption & Decryption:

aes_encrypt & aes_decrypt is used for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt it.

File Upload:

Owner uploads file into database and with the help of this metadata and its contents, it is been downloaded by user and as its encrypted it has to be decrypted.

File Download:

Authorized users can only download the file.

Cloud Service Provider Registration:

If a cloud service provider (maintainer of cloud) wants to do some cloud offer, they should register first.

Cloud Service Provider Login:

After logged in, user can see Cloud provider can view the files uploaded by their clients. This file is to be uploaded to cloud.

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 .CLOUD SERVICE PROVIDER is verified.

D. 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

Tool: Net Beans 7.1

Database: SQL Server 2005 / MySQL and hardware requirements consisting of multiple user terminals, cloud environment and required computing servers.

E. Risks Analysis of Proposed Model

RMMM plan tackles risk through Risk 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:

- ✓ Catastrophic 1
- ✓ Critical 2
- ✓ Marginal 3
- ✓ Negligible 4

Table 1. Risk Analysis of Proposed System

No.	Risk	Category	Probability	Impact
1	Increase of work load	Personal	20%	3
2	Inexperience in Project software environment	Technical	25%	3
3	Overly optimistic schedules	Project	20%	3
4	Lack of sufficient research	Technical	50%	3
5	Modules require more testing and further implementation work	Project	50%	2
6	Inconsistency in Input	Project	30%	3

CONCLUSION

In this work, It has been identified and studied a new privacy challenge during data accessing is to achieve privacy-preserving access authority sharing in Cloud Computing environment. Authentication is to guarantee data confidentiality and data integrity. The wrapped values are exchanged during transmission as Data anonymity is attained. User privacy is maintained and intact by anonymous access requests to inform the cloud server about the users' access desires privately. Security is realized by the session identifiers and the session correlation is prevented. It indicates the studied scheme is applied for enhanced privacy preservation for cloud applications. It is the main and big need in IT industries to secure their cloud access as well as expand their business to massive consumer communities to gain the profit from this technology.

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.

ACKNOWLEDGEMENT

The authors would like to acknowledge Computer Engineering department, SITRC and all the people who have given their direct and indirect contribution for providing the facilities being required for this review paper.

REFERENCES

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

[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 Zhibin Chen, 2010 Cloud Computing Research and Security Issues", In 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.

[6] Krešimir Popović and Željko Hocenski 2010 Cloud computing security issues and challenges, In MIPRO.

[7] Farhan Bashir Shaikh and Sajjad Haider,2011, Security Threats in Cloud Computing, In 6th International Conference on Internet Technology and Secured Transactions.

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

[9] Midya Azad Ismail, Klinsega Jeberson,"Secure Data Sharing Through Cloud Computing", In International Journal of Computer Engineering & Technology(IJCET), 2014,vol. 5, pp. 41-47

[10] Hong Lui, Huansheng Ning, Qingxu Xiong, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transaction, vol. pp no. 99, 2014.
[11] Debajyoti Mukhopadhyay, Gitesh Sonawane, 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

AUTHOR'S PROFILE

	Author's Name : **Madhumita S Patil** Is pursuing the Masters in Computer from Sandip Institute of Technology and research Centre, Nasik under Pune University. She has pursued her Bachelor's Degree in Computer from S.S.V.P.S.C.O.E Dhule, North Maharashtra University.

	Author's Name : **Prof. Santosh Kumar** Completed his M.Tech CSE. He is working as Professor in SITRC college of Engineering, Nashik, Maharashtra.