International Conference on "Emerging Trends in Computer Engineering, Science and Information Technology"-2015
Special Issue of International Journal of Electronics, Communication & Soft Computing Science and Engineering, ISSN: 2277-9477

Performance Enhancements in Cloud Server Using Trusted Third Party and AES

Madhumita S Patil **Prof. Santosh Kumar**

***Abstract* — Cloud computing is continuously developing as a predominant data interactive standard to realize users' data remotely stored in an online cloud server. Cloud services provide great amenities for the users to enjoy the on-demand cloud applications without considering the local groundwork boundaries. During the data retrieving, different users may be in a cooperative relationship, and thus data distribution becomes substantial to achieve creative benefits. Though the user's data is not accessed by unwanted sources, the other's data is exposed to risk by request for sharing. The user's privacy is at risk as the access request may reveal all the information. In this paper, we propose privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storing and also trying to address to the efficiency increased by this SAPA protocol. In the SAPA, 1) shared access right is achieved by anonymous access request equivalent mechanism with security and secrecy considerations 2) attribute based access control is adopted to realize that the user can only access its individual data fields; 3) alternative re-encryption is applied by the cloud server to deliver data sharing among the multiple users. It also designates that the proposed protocol realizing privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications.**

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" [3]. 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 [4]. 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 realize 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, the 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[6].

Data security is important in cloud computing. To achieve this we are using secure data access model which has some problems. So we are proposed one system which will do the task of system manager to sustain the advantages of proposed approach. So this task is done by third party auditors[10].

II. RELATED WORK

A number of different mechanisms have been proposed and implemented for privacy preservation. Few have been referred:

Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan [5] address capability based access control technique that ensures only valid users will access the outsourced data. The authors also propose a modified Diffie-Hellman key exchange protocol between cloud service provider and the user for secretly sharing a symmetric key for secure data access but key management and distribution scenarios are not mentioned.

Zhidong Shen, Qiang Tong [6] proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. In this model, some important security

services, including authentication, confidentiality and integrity are proposed in cloud computing system but there is no mention for data integration

Weichao Wang, Z. Li, R. Owens, and B. Bhargava [7] propose to encrypt every data block with a different key so that flexible cryptography-based access control can be achieved. Through the adaptation of key derivation methods, the owner needs to maintain only a few secrets but scheme for key management is not mentioned.

Privacy Preserving Data Sharing With Anonymous ID Assignment

An algorithm use a technique to assign the nodes ids allowing more complex data to be shared and has applications to other problems in privacy preserving data mining, collision Avoidance. The work has done on the non cryptographic algorithm[4]

III. METHODOLOGY

The proposed system consist of the following main actors Cloud Service Provider (CSP) , users, owner of the data and Trusted Third Party (TTP).

The Owner of the data is placed on the cloud and the user can access if the access control has been given by the Owner. When the access permission has given by the Owner the AES come into picture. The private and the public has been generated. Only using these keys encryption is done. When the user is intended to access the files from the cloud server it has decrypt using the private key.

When a new user is going to register, during the registration only it has to choose the owner and the same access request is sent to the Data owner. Then the owner accepts request and grant the permission. And hence the user will be able to access the File uploaded by the user.

Now the question is where the TTP is performing its role. It performance purely the authentication and the validation of the new user accessing the file from the cloud. When the new user registers, there's one mechanism performed by TTP, it keeps track of newly added user. It sets the value in db as the not registered and need confirmation. The verification and authentication is done by sending the OTP on the email id of the user. When the user clicks on the Generate OTP and enters in the verification box then only the value is set as verified user in DB by TTP.

Owner has to send capability list and an encrypted message for user with all the key parameters which are needed by user for decrypting the data files. Once the Keys have been available to the user data access request is sent to Cloud Service Provider and hence after the authorization the data is available to the user [11].

The following is the Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing which explains how the actual implementation of the proposed system [8] :

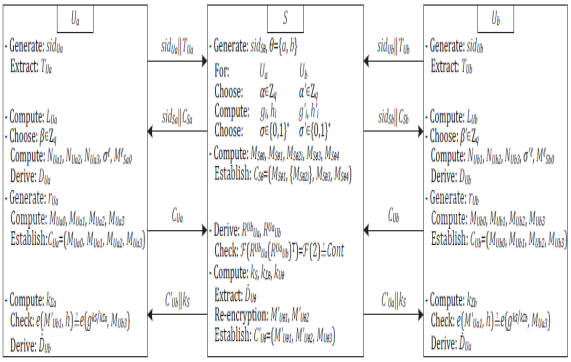

Fig 3.1: System Initializations and the implementations

V. ANALYSIS MODEL

The performance analysis is done with respect to the enhancements over the existing systems.

The existing system is implemented without use of the TTP. But when it is compared with the TTP and AES implementation the performance is said to be increased.

AES can be said to the efficient algorithm as [10]:

	AES	DES
Type of Algorithm	**Symmetric , block cipher**	**Symmetric , fiestel cipher**
Key Size (in bits)	**128,192,256**	**112,168**
Speed	**High**	**low**
Time to crack (250 keys per second)	**149 trillions**	**46 billion years**
Resource consumption	**low**	**Medium**

Table 3.1: File download time measure

DES has following limitation which will be overcome by AES:

1) Really old technology
2) Easily breakable
3) Smaller key size
4) Smaller block size
5) Uses Feistel Strucuture

The Non-ttp system is surveyed found following drawbacks:

• Key generation/distribution: Every time a user encrypts a file, she has to generate a unique symmetric encryption key with the help of client application downloaded from cloud or using the one selected on her own. For a non-technical user, this may be little confusing operation during initial phase of cloud utilization.

• Performance: This is one of the main issues to be discussed with non-TTP approaches. The soft approach to perform cryptographic computing & communication operations may be as fast as compared to specially designed dedicated extra hardware

in form of TTP for resource consuming cryptographic operations. Though one may perform these operation offline, to possible extent, to improve performance.

• Multiple task handling & Batch Auditing: Dedicated TTP is specialized in handling multiple task handling and bath auditing issues. The client application may not give the same performance as TTP with available computing resources in presence of other applications running on client machines.

Hence, the trusted Third party is preferred over the Non-TTP using AES the functionality seems more promising.

VI. RESULT

The implementation and the observation from the implemented proposed system , this is observed that the load balancing is done using the Trusted third party as it does the verification and authentication of the user accessing the data.

Also, the TTP,Key generation and the SAPA protocol ensures the data is secured and will not be accessed using any other unwanted user.

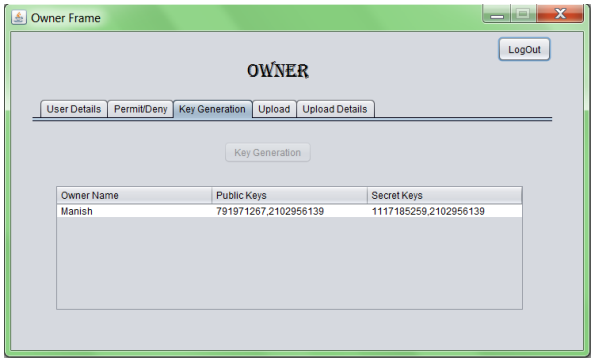

FIG 4.1 : Owner Key Generation

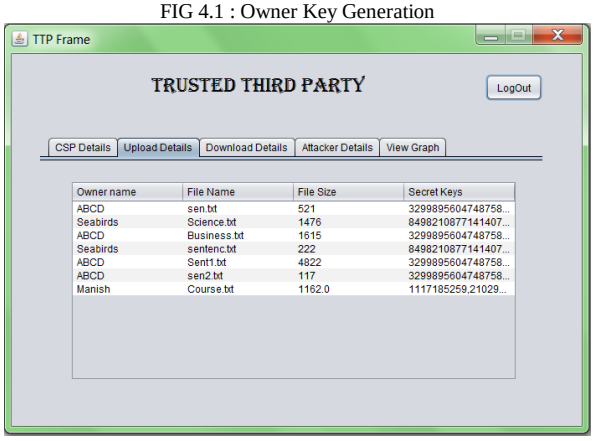

Fig 4.2 : Trusted Third Party Verification

CONCLUSION

The proposed work has identified and tends to work on User Privacy, Data anonymity and the Authorisation for the data sharing. The basic behind achieving this feature is data is wrapped and then exchanged between each other. And also, the access request is privately conveyed to the cloud server. Through the trusted third party we will remove the overhead to the server.

ACKNOWLEDGMENT

We find great pleasure in expressing our deep sense of gratitude towards all, who have made it possible for us complete this Paper Preparation with success.

We are thankful Prof. Amol Potgantwar HOD of Department of Computer Engineering, SITRC .They have always been supportive and helpful throughout the course of Master of Engineering.

REFERENCES

[1]. Rich Maggiani, 2009 Cloud Computing Is Changing How We Communicate", In IEEE 978-1-4244-4358-1/09. [2]. Yujin Li, Ming Zhao, Wenye Wang ,"Intermittently Connected Vehicle-to-Vehicle Networks: Detection and Analysis", 2011 IEEE

[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] Larry A. Dunning and Ray Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transaction ,vol.8,pp.2, Feb.2013

[5]. Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan, "Secure data Access in Cloud Computing",in 4th International conferenceon Internet Multimedia ServicesArchitecture and Application(IMSAA),2010 IEEE.

[6]. Zhidong Shen, Qiang Tong, "The Security of Cloud Co mputing System enabled by Trusted Computing Technology", in second International Conference On Signal Processing Systems, 2010 IEEE

[7]. Weichao Wang, Z. Li, R. Owens, and B. Bhargava, "Se cure and efficient access to outsourced data," in P roc. of ACM Cloud Computing Security Workshop, pp. 55-65, 2009

[8]. Hong Liu,Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing, IEEE Transaction on Parallel and Distributed System Vol:pp No:99 YEAR 2014

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

[10]. http://web.townsendsecurity.com/bid/72450/What-are-the-Differences-Between-DES-and-AES-Encryption

[11]. R.S.Nejkar and G.S.Patil "Trusted Third Party Service For Secure Cloud Data", IJRET,vol.2,June 2014,203-210.

AUTHOR'S PROFILE

Madhumita S Patil

Currently studying in Sandip Institute of Technical and Research Centre ,Nasik, Savitribaii Phule university of Pune, Pune.
M.E.(Computer 2nd Year)