ISSN:0975-9646

Snehal Vilas Zargad et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4062-4064

Data Integrity Checking Protocol with Data Dynamics and Public Verifiability for Secure Cloud Computing

Snehal Vilas Zargad[1], Amruta Vijay Tambile[2],Shivangi Shashikant Sankoli[3], Rajashree Chandrakant Bhongale[4]

Department Of Information Technology
Dr. D. Y. Patil Institute of Engineering and Technology
Ambi, Pune, India

***Abstract* – In the concept of cloud computing the main actor is Third Party Auditor. In this paper we propose method to eliminate the Third Party Auditor from cloud computing which mainly checks whether the user which is using the cloud services is authorized or not. Here we will try to come up with new service which is capable removing the most of threats occur in the normal working of cloud computing. In contrast to conventional solutions, which are well protected by standardized data access procedures, organizations tend to lose integrity of data when the systems are outsourced to cloud. Since the data is stored they must ensure to overcome threats occurring in the cloud. Our proposed system includes the new concept of dynamic encryption. In dynamic encryption the encryption algorithm type is decided dynamically depending upon the type of data as well as the size of data.**

Keywords: Cloud computing, Third Party Auditor, Threats in cloud computing, dynamic encryption.

I. INTRODUCTION

Cloud computing is the hottest topic in the technology and industry. The cloud computing is the concept of delivery of computing as a service rather than product, the computer resources, software and information shared instead of other devices.

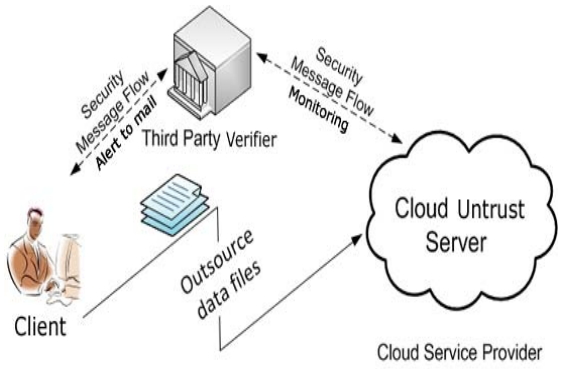

Fig. 1 Actual Cloud scenario

In the idea of cloud computing the user of cloud outsources its data on to the cloud, and then the third party auditor is going to check authorization of that user to access the cloud. In cloud if it is found that the unauthorized user is trying to access data of any other authorized user then the third party comes in picture, the third party auditor gives the notification to the authorized user that some unauthorized user is trying to access its private data. The concept of cloud computing represents a shift in thought, in that end users need not know the details of a specific technology. The service is fully managed by the provider. This on demand service can be provided at cloud service providers are making a substantial effort to secure their systems, in order to minimize the threats of insider attacks, and reinforce the confidence of customers. In the cloud scenario if third party auditor itself get hacked then the authorized will not receive any notification of unauthorized access of its data. So in the propose method the service will eliminates the third party auditor.

II. LITERATURE SURVEY

Mr. Prashant Rewagad and Yogita Pawar suggested that Cloud Computing could be defined as utilizing the internet to provide technology enabled services to people and organizations [1].The advantages for using cloud computing are Reducing capital expenditure, operational risk, complexity, maintenance and increase scalability. They propose diffie-hellman key exchange blended with advance encryption standard algorithm and digital signature but in future they faced the problem that if key in transmission is hacked then diffie-hellman key exchange is useless.

Some researchers have suggested that user data stored on a Service-provider's equipment must be encrypted. Encrypting data prior to storage is a common method of data protection, and service providers may be able to build firewalls to ensure that the decryption keys associated with encrypted user data are not disclosed to outsiders. However, if the decryption key and the encrypted data are held by the same service provider, it raises the possibility that high-level administrators within the service provider would have access to both the decryption key and the encrypted data, thus presenting a risk for the unauthorized disclosure of the user data.

Existing methods for protecting data stored in cloud environment are user authentication, building secure channel for transmission of data. For this procedure they uses various Cryptographic as well as Security based algorithm such as AES(Advance Encryption Standard),DES(Data Encryption Algorithm),Triple DES, RSA algorithm with digital signature.

Prof. Gajendra Singh had suggested that a method to build trusted computing environment for cloud computing system by integrating a trusted computing platform into the security of cloud computing system. They had proposed a model system in which a cloud computing system is combined with trusted computing platform with trusted platform module. In their proposed model some important security services, including authentication,

confidentiality and integrity, are provided in cloud computing system.

Ms. Gargee Sharma, Ms.Prakriti Trivedi had proposed a model which separating a Encryption-Decryption service from the actual cloud storage. Because of this the data and decryption key will be at different so the attacker will get either encrypted data or decryption key. This tends to provide extra level of security. In their proposed model the Encryption-Decryption service will only the encrypt the data and this encrypted data is send to cloud storage and then original data is deleted from Encryption-Decryption service.

In the existing system the main role of authentication of user is done by TPA, the TPA verifies the user whether it is valid user or not. If the user is not authorized then the TPA notify to the user that his data is used by some unauthorized person. But if the TPA itself get hacked then the user will not get an notification mail from TPA. Authentication and verification is done at TPA level and not at admin level. In existing cloud system, there are no of threats occurred and they are as follow:

1) Abuse and Nefarious use of cloud.
2) Insecure Interfaces and APIs.
3) Malicious Insider.
4) Shared Technology Issues.
5) Data Loss and Leakage.
6) Account or Service Hijacking

III. PROPOSED SYSTEM

In this paper we are coming with a model of service which will eliminate the TPA from the cloud scenario. And our proposed service will be capable of handling the all work of TPA. At the time of data modification or uploading a new data the service will generate a password using 3D colour logic and that password will be sent to him by mail, by giving this password only the user will be able to proceed further.

The proxy server is act as administrator, whenever user try to access data in read only mode then the user can access directly from cloud without interacting with administrator, and if the user want to insert, modify or delete data then the notification of this will sent to the administrator. While for the first time data inserting the Encryption service generate encryption key and this key is stored separately on Key Storage area, and encrypted data is stored on the cloud storage area.

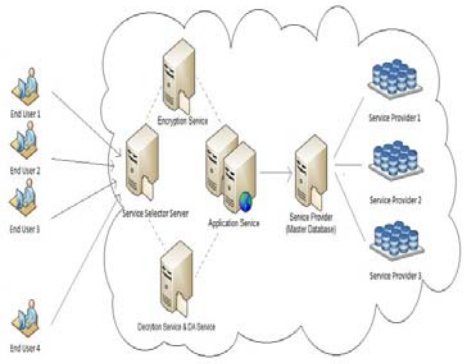

Fig. 2 System Architecture

In decryption process when the user request for the data, then key and data are collected at the Decryption service but the service will not immediately decrypt the data, until and unless user insert the OTP sent on his mail. When user will enter this OTP correctly then the data is decrypted by Decryption service and data is provided to the user.

IV. ALGORITHMS

Mainly two algorithms are used in the system, namely, AES and RC6. AES is used for File Encryption and Decryption. RC6 is used for Message Encryption and Decryption.

A. AES Algorithm

The algorithm used in the system is AES algorithm which is a symmetric key block cipher with 128 bit block length. It uses same key for encryption as well as decryption of information. The size of cipher text produced is same as the plain text. Operations in AES is mostly done on the basis of bytes. It is based on the design principle substitution permutation network. Internally, AES algorithm's operations are performed on two-dimensional array of bytes called array. Following are the steps followed in AES algorithm:

1) SubByte – The substitution of each byte is done through S-Box. These are transformed using a non-linear but invertible S-Box.
2) ShiftRows- A permutation which cyclically shifts last three rows in the state. Left shift of number of bytes is equal to the row number.
3) MixColumns –It is a substitution that used GF(Galois Fields) arithmetic. It interpret each column as a vector of 4. Each column of state is replaced by another column obtained by multiplying that column with matrix in particular field.
4) AddRoundKey – there is bit by bit XOR with expanded key.

Due to a several number of advantages, AES algorithm provides the best way to encrypt any data. It provide high security, flexibility, simplicity and most important it has a reasonable cost. It is resistant to linear and differential cryptanalysis. The attack is not practically possible due to several rounds in algorithm. It is efficient for hardware and software both across various platforms.

B. RC6

RC6 is a block cipher. It is an evolutionary improvement of RC5, designed to meet the requirements of the Advanced Encryption Standard (AES). Like RC5, RC6 makes essential use of data-dependant rotation. New features of RC6 includes the use of four working registers instead of two, and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication greatly increases the diffusion achieved per round, allowing for greater security, fewer rounds, and increased throughput.
There are three Round Stages used in RC6

1) Pre-whitening – Removes inference of part of the input to the first round of encryption.
2) r rounds- It uses integer multiplication as well as quadratic equation [f(x)=x(2x+1)(mod 2^w)] . It also uses fixed bit shifting. All of the above are required for sufficient diffusion
3) Post-whitening – Removes inference of part of the input to the last round of encryption.

V. IMPLEMENTATION

The system is can be implemented on any Microsoft Windows environment. It can be operated on any web browser and will have conformity with Mozilla, Opera, Internet Explorer, Netscape Navigator. SQL Server 2005 and .NET 4.0 is used as a base for the system implementation. The system specification contains 400 GB hard disk capacity, 2 GB RAM, Intel processor 2.0 GHz. Using all these components, the system is executed successfully.

VI. SYSTEM FEATURES

We propose a service in which the existing cloud threats are eliminated by-
Step 1: Encrypted data and key are stored separately on different storage media.
Step 2: Before decrypting the data the user have to enter OTP which is sent on his mail and combination of OTP, key and encrypted data are used to generate original data.
Step 3: For accessing the data the user is restricted in read only mode and for insert, modify and delete the notification is sent to admin.
Step 4: After encryption or decryption the original data is deleted from the Encryption and Decryption services.
Step 5: For securing the Account and Service Hijacking, we are eliminating the TPA.

The work of TPA will be done by admin and Our propose system.

VII. APPLICATIONS

A. *Enterprise Resource Planning*

Enterprise Resource Planning (ERP) systems are also capable of integrating all of a company's departments and functions onto a single computer system to serve all needs. But, generally, ERP is not perceived as innovative technology. At best, most executives view ERP as a double-edged sword — a one-time rite of passage that must be performed in order to remain competitive.
When Web computing and ERP are combined, though, it is important to conduct a sober evaluation of the costs and risks involved to ensure desired benefits do not go up in smoke.

B. Customer Relationship Management

For any company looking to improve its customer relationship management, or "CRM," needs, implementing a CRM Web computing system is both efficient and cost effective. Delivering a sales team a blend of unique functionalities to improve agent/customer interactions, a CRM Web computing system will never be limited by underlying technology. A CRM Web computing platform helps a company track any data, such as orders, discounts, references, competitors and much more. Since salespeople need to route orders and service agents need to validate customer entitlements, with a CRM Web computing platform, a company can run code in the Web so there are no limitations on creating CRM logic.

VIII. CONCLUSION

In this paper, we examine the threats in cloud system and with our proposed service we are eliminating these threats. We also had studied the dynamic encryption and we are proposing to be implement in our service. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

IX. FUTURE SCOPE

A Proposing module study of data security with respect to data leakage, fake profile, insecure interface and their factors. Rest network base security threats like Distributed Denial Of Service(DDOS) attack, Bruit force attack are to be target in future enhancement.

ACKNOWLEDGMENT

We take this opportunity to thank our project guide Prof.Anirban Dutta and Head of the Department Prof. Mr. Amol Jadhao And Principal Dr. R. J. Patil for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of Dr. D. Y. Patil Institute of Engineering and Technology, Ambi for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books..

REFERENCES

[1] P. Mell, T. Grance ,"Draft NIST working definition of cloud computing", [Online]Available: http://www.csrc.nist. gov/groups/SNS/cloud-computing/index.html
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz,A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica,M. Zaharia,"Above the clouds: A berkeley view of cloud computing", University of California, Berkeley, Tech. Rep.UCB-EECS-2009-28, Feb 2009.
[3] N. Gohring (2008),"Amazon's s3 down for several hours",[Online] Available: http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html
[4] Amazon.com (2008),"Amazon s3 availability event: [Online]Available: http://wwwstatus.aws.amazon. com/s3-20080720.html
[5] S. Wilson (2008),"Appengine outage", [Online] Available:http://www.cio-weblog.com/50226711/appengine outage.php.