Efficient Security Solution for Privacy-Preserving Cloud Services

Priyanka[1]
Student, KITM,
Kurukshetra, India

Sunil Saini[2]
Assistant Professor, KITM,
Kurukshetra, India

Abstract— **The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies In this paper, we present a novel privacy-preserving security solution for cloud services. We deal with user identification and secure communication. Our solution provides only registered users to access cloud services. Our solution offers anonymous authentication. This means that users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity. Our solution offers secure communication of transmitted data.**

Keywords— Authentication, Cloud Computing, Cryptography, Encryption, Privacy, Security.

I. Introduction

The cloud computing becomes the host issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. It is based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability. The resource in the cloud system is transparent for the application and the user do not know the place of the resource. The users can access your applications and data from anywhere. Resources in cloud systems can be shared among a large number of users. The cloud system could improve its capacity through adding more hardware to deal with the increased load effectively when the work load is growing. Cloud resources are provided as a service on an as needed basis. The cloud itself typically includes large numbers of commodity-grade servers, harnessed to deliver highly scalable and reliable on-demand services. The amount of resources provided in the cloud system for the users is increased when they need more and decrease when they need less. The resource can be the computing, storage and other specification service. The cloud computing is seen as the important change of information industry and will make more impact on the development of information technology for the society. There are few cryptographic tools that can both hide user identity and provide secure communication. The providers of cloud services need to control the authentication process to permit the access of only valid clients to their services. In practice, hundreds of users can access cloud services at the same time. Hence, the verification process of user access must be as efficient as possible and the computational cryptographic overhead must be minimal. We propose a novel security solution for cloud services that offers anonymous authentication. We aim mainly on the efficiency of the authentication process and user privacy. Our solution also provides the secure communication and privacy of transmitted data between users and cloud service providers. Our results show that our solution is more efficient than the related solutions.

The paper is organized as follow: The next section presents the related work. In section 3 we introduce our novel privacy-preserving security solution for cloud services. Section 4 contains our experimental results. Finally, the conclusion of our work is presented

II. Related Work

Privacy-preserving cloud computing solutions have been developed from theoretical recommendations to concrete cryptographic proposals. There are many works which deal with general security issues in cloud computing but only few works deal also with user privacy. The authors [1] explore the cost of common cryptographic primitives (AES, MD5, SHA-1, RSA, DSA, and ECDSA) and their viability for cloud security purposes. The authors deal with the encryption of cloud storage but do not mention privacy-preserving access to a cloud storage The work [2] establishes requirements for a secure and anonymous communication system that uses a cloud architecture (Tor and Freenet). Nevertheless, the author does not outline any cryptographic solution. Only validate user can write on the cloud and invalid user doesn't get access to the cloud this work is presented in paper [3]. Another cryptographic solution ensuring user privacy in cloud scenarios is presented in [4]. The authors propose an algorithm which reduces the risk of the leakage of user private information. The authors of paper [5] presented a onetime password to authenticate the users. This paper presents a secure structure to the cloud. The issue of data security is one of the most important problems to be solved in paper [6].

III. Our Solution

In this we introduce our security solution for privacy-preserving cloud services. We outline our system model, security requirements, architecture and algorithm.

A. Model of our System

Our solution consists of two fundamental parties:

- Cloud Service Provider (CSP). CSP manages cloud services and shared storages. CSP is usually a company which behaves as a partly trusted party. CSP provides cloud services, authenticates users when they access a cloud service. CSP also issues access attributes to users. Nevertheless, when CSP needs to revoke and identify a malicious user then CSP must collaborate with a revocation manager.

- User (U). U is an ordinary customer who accesses into a cloud and uses cloud services, shared storages, etc. Users are anonymous if they properly follow the rules of CSP. To increase security, users use tamper-resistant devices or protected local storages.

B Necessity

- Anonymity. Every honest user stays anonymous when uses cloud services. User identities are hidden if users behave honestly and do not break rules.
- Confidentiality. Every user's session to CSP is confidential. No one without a secret session key is able to obtain data transmitted between U and CSP.

C. Proposed Architecture

This proposed architecture is enhanced security model for cloud services like data storage. It consist of CSP i.e. Cloud Service Provider and user's.

- Cloud Service Provider: - CSP generates a pair of keys i.e. secret key and public key by using cryptography algorithm RSA. CSP stores its own private key generated RSA algorithm and public key is shared by all.
- User's:- User's must physically register on CSP. CSP check user's id. If user is already registered then there are some messages exchanged between users and CSP for establishing secure communication between them. User's generated a random request and encrypts this random request with the RSA public key of CSP and sends this request message to the server. Now server verifies this request if it is verified then server decrypt this message by using RSA secret key of CSP and generate a random key K_sym. Now with the help of this random key server generates a response by applying the X-OR operation to random and K_sym. Server send this response to user's. User's use this random key for file uploading and downloading and attain secure communication

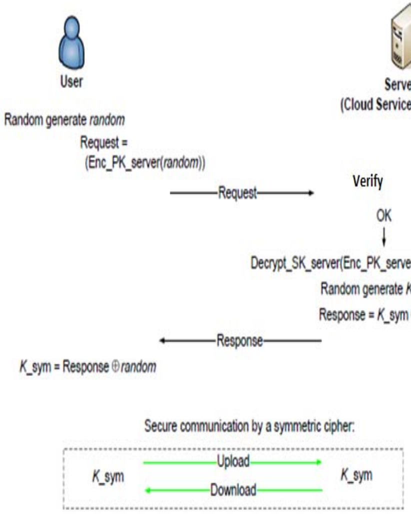

Fig 1: Architecture for proposed protocol

D. Proposed Algorithm

- Key Generation: - The CSP generates the random key pair (Pk, Sk). Two large prime numbers P, Q are generated such that N=PQ (N is 1024 bits) and φ= (P-1)(Q-1) Select a random number 1<e<φ such that gcd (e,φ)=1. Compute the unique integer $d=e^{-1}$(mod φ (n)). Where Pk (e, N) is the Public Key and Sk (d, N) is the Secret Key.
- Secure Communication: - RSA provides the secure communication between client and server. Users encrypts random by the RSA public key of CSP. The encrypted Enc PK server (random) is send to the server. Server verifies the encrypted Enc PK server (random) if it verify then the server decrypt this with its secret key and generate random key *K*_sym. Compute the Response = *K*_sym random. CSP sends a response message (random K sym) back to user.
- File Upload and Download:-The user can upload and download data to CSP. Data privacy are secured by a symmetric cipher. We propose to use AES which is well known cipher and is supported by many types of software and hardware platforms. To encrypt and decrypt transmitted data, User and CSP use the AES secret key K sym established in the previous phase.

IV. Experimental Results

In this section, we outline the experimental results of our solution. We compare our solution with related solutions and output the performance evaluation.

Table 1:-Performance Evaluation of our solution

File	**Encryption Time**		**Decryption Time**		**Total Time**	
	AES	RSA	AES	RSA	AES	RSA
16116	.229	0.284	.229	0.284	0.458	0.568
14597	0.145	0.210	0.145	0.210	0.290	0.420
12908	0.109	0.170	0.109	0.170	0.218	0.340

A. Performance Evaluation of Our Solution

We have implemented our proposed solution in ASP.net. In practice, we expect that U as an end node uses devices with reasonable computational power such as a personal computer, a laptop, a tablet or a smart phone. On the other hand, we assume that CSP keeps servers with sufficient computational capacity to ensure hundreds sessions with end nodes in real time. We have tested our solution on a machine with Intel(R) Xeon(R) CPU X3440 @ 2.53GHz, 4 GB Ram. The main important part of our solution is the Anonymous Access phase. In this phase, a user (U) communicates with a Cloud Service Provider (CSP). The computation process on the user side is marked as the Sing/Authenticate process. The computation process on the CSP side is marked as the Verify process. We have measured the total time of the Sing/Authenticate process and the Verify process. The main concern of our dissertation is to attain privacy of data so to attain the privacy of data we have to store our data contents in encrypted format over cloud. We have to measure this estimated encryption decryption time. When we measure the experimental results we shows that estimated encryption /decryption time is less in proposed system than in existing system. This shows that our solution is more efficient than existing system When we compare our result with existing result on the same size of file we find that our result is more efficient than the existing work in terms of time delay.

B. Comparison with Related Work

We compare our Anonymous Access phase with the authentication phase of related solutions we find that our solution is better than in terms of encryption/decryption time and also to attain privacy.

The time taken by our solution for encryption and decryption is less as compared to existing when we test the same file size.

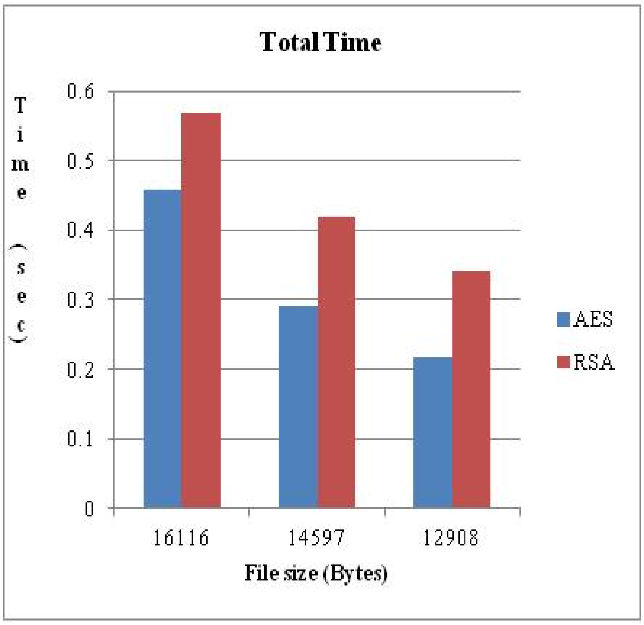

Fig 2: File Size vs. Total Time Taken

V. CONCLUSION

The paper presents solution which offers user anonymity in authentication phase and confidentiality during file uploading and downloading for all users. Our authentication phase is more efficient than related solutions on the client side and also on the server side due to missing expensive bilinear pairing operations and fewer exponentiation operations. Due to this fact, cloud service providers using our solution can authenticate more clients in the same time. We deal with user anonymous access to cloud services and shared storage servers. Our solution provides registered users with anonymous access to cloud services.

The future perspectives for this paper is to use some another cryptography algorithm so that the system take minimum encryption time and decryption time to conclude the estimation time also we can use any other operation so that we can enhance the secure communication between user and cloud service provider.

REFERENCES

[1] Y. Chen and R. Sion, “On securing untrusted clouds with cryptography,” in Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. ACM, 2010, pp. 109–114.

[2] R. Laurikainen, “Secure and anonymous communication in the cloud,” Aalto University School of Science and Technology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10, 2010.

[3] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds”in proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

[4] Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal.” Enhanced Security for Cloud Storage using File Encryption” Department of Information Technology Maharashtra Institute of Technology

[5] Kawser Wazed Nafi1,2, Tonny Shekha Kar2, Sayed Anisul Hoque3, Dr. M. M. A Hashem4, “ A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”in proceeding of the (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2011

[6] Du meng.” Data security in cloud computing” in yhe proceeding of the The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka

[7] Hamid Banirostam, Alireza Hedayati, Ahmad Khadem Zadeh and Elham Shamsinezhad.” A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure” 2013 UKSim 15th International Conference on Computer Modelling and Simulation