Survey on Cloud Security
Mechanisms for Data Storage and Data Transaction

Kavitha.K*1, Saravanan.V*2

*1 Department of Computer Applications , Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India
*2 Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

Abstract—Cloud computing is an Information Technology model which allows all time access to shared pools of system resources and services from anywhere at reduced effort and cost. Cloud computing decreases the hardware and software demand for the users. Cloud storage is an important service of cloud computing. It offers low cost, on-demand large storage and processing resources. Security is an essential barrier to cloud computing. Security need to be concentrated and prioritized in cloud environment during data transmission and storage. A user’s data is stored in the cloud servers. Only authenticated users are allowed to access the data in the cloud. To improve cloud security, many authentication techniques are used. Authentication accuracy and data confidentiality of existing methods are not up to the expected limits. The main objective of our work is to improve the level of security during data transmission and storage through cryptographic techniques.

Keywords—Cloud computing, data storage, data transmission, data confidentiality, security.

I. INTRODUCTION

Cloud computing provides ubiquitous access to the resources. This highly scalable cloud computing environment offers software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) to the companies and individuals and hence forth became the source of future computing. The data stored in the server is safeguarded by the process of storage security. Unauthorized users are prevented from accessing data from the server by the process of authentication. When data is transmitted between users, it is protected by the process of transaction security.

This paper is organized as given below: Reviews on authentication techniques for secure data transmission and storage is described in Section 2, existing authentication techniques are explained in Section 3, a comparative study among them is described in Section 4, limitations are given in Section 5 and conclusion of the paper is given in Section 6.

II. REVIEW ON RELATED WORKS

Two-factor security protection mechanism was presented in [1] with factor revocability for cloud storage. Here the sender encrypts the messages and sends them to the receiver through the cloud server. But at the receiving end the cipher text could not be decrypted if the device is lost. Hence this method could not enhance the security level. In [2] a new secure cloud storage system with time-based one-time password and automatic blocker protocol was implemented to protect the system from unauthorized third party auditor. But, when auditing the shared data integrity, the efficiency of the system could not be improved.

A new public auditing scheme with dynamic hash table (DHT) was introduced in [3] for secure storage in cloud. This scheme used homomorphic authenticator based on public key with random masking created through third party auditor (TPA), to improve the privacy preservation. But still secure auditing could not be achieved. In [4] a quantum identity-based authentication and key agreement scheme for cloud server architecture was designed. AVISPA tool was used to make the security analysis. But, this protocol leaked information to the verifier. So, quantum identity-based authentication and key agreement scheme could not improve security level as well as the data integrity rate.

To reduce the cost and complexity for managing the public key, an identity-based remote data integrity checking with key-homomorphic cryptographic model was introduced in [5]. Even though this protocol does not leak information, the authentication time was not minimized. To enhance the association in cloud, in [6] an extendable access control system with integrity protection using functional key encapsulation with equality testing was implemented. But, no integrity protection was done to extend the access policy.

To have an authorized access to information in the distributed cloud, a light weight authentication protocol was implemented in [7]. But, this protocol failed to enhance authentication accuracy.

III. AUTHENTICATION TECHNIQUES FOR SECURED DATA TRANSACTION AND DATA STORAGE IN CLOUD

Cloud computing is a data-centric network service model used for data storage, data sharing, bigdata organization and medical information systems. Cloud computing is the future generation of distributed computing. It is a suitable model for on-demand network access to computing resources with very less effort. Authentication is an essential factor in cloud. There are many authentication techniques to restrict access in cloud.

A. Two Factor Data Security Mechanism for Cloud Storage

Two-factor security protection mechanism was introduced with factor revocability for cloud storage. Here the sender encrypts the messages and sends them to the receiver through the cloud server. The sender needs to be aware of only the
identity of the receiver and nothing more than that. But, the receiver need to know the secret key and the unique personal security device to decrypt the cipher. The secret key is stored in the computer and the unique personal device is linked to the computer.

This mechanism is an identity based encryption. The sender needs to know the identity of the receiver alone for transmitting the encrypted data. The sender sends the encrypted information to the cloud server, from where it can be downloaded by the receiver any time. The receiver could decrypt the encrypted information only with the help any one of the two things. However at the receiving end the cipher text could not be decrypted if the device is lost. This process is transparent to the sender.

B. Public Auditing using Dynamic Hash Table for Secure Storage

Enterprises and individuals use cloud data centers to store and access their data remotely without any burden. By outsourcing data, the cloud users are mitigated from local data storage and preservation. The cloud storage is used by the cloud users like a local storage without worrying about the data integrity and consistency. A special person called the third party auditor is employed in cloud computing to verify the stored data in the cloud. The third party auditor is leased by the cloud service provider and thus can prevent the defamation by hiding the data loss from the users.

A new public auditing scheme was presented for secure cloud storage depending on dynamic hash table. The dynamic hash table was a two dimensional data structure at third party auditor to record data property information for auditing. The designed scheme minimized the computational cost by transferring the authorized information from the cloud service provider to the third party auditor. It also offers high updating efficiency with reduced computational overhead. In this scheme, privacy preservation was done using homomorphic authenticator depending on public key with random masking generated by third party auditor. This scheme also used Boneh Lynn Schacham signature and bilinear maps for attaining batch auditing. Thus the public auditing scheme performed dynamic auditing, privacy protection and batch auditing. The dynamic hash table collects the data properties for auditing in third party auditor.

C. Identity based Secure Authentication scheme using Quantum Key Distribution for cloud computing

Authentication is the process of identifying the legitimate user through validating credentials provided by the user. It is an important part in integrating the devices and the cloud service providers. The two parties construct the session key through the key exchange scheme.

Now-a-days a number of hackers try to change into legitimate users to hack the sensitive data. So to prevent this, a Quantum Identity based Authentication and Key agreement scheme is designed for the cloud server architecture. To secure privacy and confidentiality, quantum physics laws are used in Quantum Cryptography. AVISPA tool was used to carry out the security verification.

The user who wants to access a cloud service, is verified for his identity using a new authentication scheme. If the user is legitimate, then access to cloud service is provided, else access will be denied. This newly designed scheme combined the classical identity authentication with unconditionally secure Quantum Key Distribution and hence improved the authentication security level. This scheme used an EPR pair which is a pair of entangled quantum bits. Also information could not be saved for decryption through advanced technologies. This designed scheme minimized the number of attacks and became a robust protocol.

IV. RELATIVE STUDY OF AUTHENTICATION TECHNIQUES FOR SECURED DATA TRANSACTION AND DATA STORAGE IN CLOUD

To compare these authentication techniques, an experiment is done on number of cloud user requests, taking into consideration various parameters like data confidentiality rate, authentication time and authentication accuracy that are used for secure cloud transaction and data storage.

A. Data Confidentiality Rate

Data Confidentiality Rate is the rate at which the data is transacted to a legitimate user without unauthorized access. It is a measure of the system’s ability to protect its data. It also guarantees that the blocks are not accessed by entities without any rights. Higher the data confidentiality rate, more efficient will be the system.

The performance of data confidentiality rate is measured by experimenting the cloud user requests ranging from 10 to 100. The following are few random sample observations:

- For 10 cloud user requests: the data confidentiality rate is 81 % for Two-factor Authentication mechanism, 65% for Public Auditing using DHT and 72% for Identity based Authentication Scheme.
- For 50 cloud user requests: the data confidentiality rate is 88 % for Two-factor Authentication mechanism, 68% for Public Auditing using DHT and 75% for Identity based Authentication Scheme.
- For 80 cloud user requests, the data confidentiality rate is 86 % for Two-factor Authentication mechanism, 74% for Public Auditing using DHT and 80% for Identity based Authentication Scheme.
- For 100 cloud user requests: the data confidentiality rate is 92 % for Two-factor Authentication mechanism, 83% for Public Auditing using DHT and 88% for Identity based Authentication Scheme.

From the experimental observations, it could be concluded that the data confidentiality rate does not get linearly increased when the number of cloud user requests gets increased. The data confidentiality rate of Two Factor Data Security Mechanism is higher than Public Auditing using Dynamic Hash Table and Identity based Secure Authentication scheme using Quantum Key Distribution.
mechanisms. Also, the data confidentiality rate of Public Auditing scheme using DHT is 20% lesser than Two Factor Data Security Mechanism and the data confidentiality rate of Identity based Authentication Scheme is 9% lesser than Two Factor Data Security Mechanism.

B. Authentication Time

Authentication time is defined as the amount of time consumed for performing the authentication process. It is measured in milliseconds (ms). Authentication time can also be measured as the difference between the starting and ending time of authentication.

\[
\text{Authentication Time} = \text{Ending Time of Authentication} - \text{Starting Time (1)}
\]

The lesser the authentication time, the more efficient will be the mechanism.

The performance of Authentication time is measured by experimenting the cloud user requests ranging from 10 to 100. The following are few random sample observations:

For 10 cloud user requests: the Authentication time is 43 ms for Two-factor Authentication mechanism, 24 ms for Public Auditing using DHT and 36 ms for Identity based Authentication Scheme.

For 50 cloud user requests: the Authentication time is 52 ms for Two-factor Authentication mechanism, 30 ms for Public Auditing using DHT and 42 ms for Identity based Authentication Scheme.

For 80 cloud user requests: the Authentication time is 50 ms for Two-factor Authentication mechanism, 26 ms for Public Auditing using DHT and 38 ms for Identity based Authentication Scheme.

For 100 cloud user requests: the Authentication time is 59 ms for Two-factor Authentication mechanism, 32 ms for Public Auditing using DHT and 45 ms for Identity based Authentication Scheme.

From the experimental observations, it could be concluded that the Authentication time gets changed when the number of cloud user requests vary. The Authentication time of Public Auditing using Dynamic Hash Table Mechanism is lesser than Two Factor Data Security Mechanism and Identity based Secure Authentication scheme using Quantum Key Distribution mechanisms. Also, the Authentication time of Public Auditing scheme using DHT is 47% lesser than Two Factor Data Security Mechanism and 33% lesser than Identity based Authentication Scheme.

C. Authentication Accuracy

Authentication accuracy is defined as the ratio of number of cloud user requests authenticated correctly to the total number of cloud user requests. Authentication accuracy is measured in terms of percentage (%), and is formulated as below:

\[
\text{Authentication Accuracy} = \frac{\text{Number of cloud user requests authenticated correctly}}{\text{Total number of cloud user requests}} \rightarrow (2)
\]

Higher the authentication, the more efficient will be the method.

The performance of Authentication accuracy is measured by experimenting the cloud user requests ranging from 10 to 100. The following are few random sample observations:

For 10 cloud user requests: the Authentication accuracy is 70% for Two-factor Authentication mechanism, 69% for Public Auditing using DHT and 82% for Identity based Authentication Scheme.

For 50 cloud user requests: the Authentication accuracy is 74% for Two-factor Authentication mechanism, 82% for Public Auditing using DHT and 90% for Identity based Authentication Scheme.

For 80 cloud user requests: the Authentication accuracy is 76% for Two-factor Authentication mechanism, 93% for Public Auditing using DHT and 96% for Identity based Authentication Scheme.

For 100 cloud user requests: the Authentication accuracy is 78% for Two-factor Authentication mechanism, 90% for Public Auditing using DHT and 91% for Identity based Authentication Scheme.

V. LIMITATIONS OF AUTHENTICATION TECHNIQUES FOR SECURED DATA TRANSACTION AND DATA STORAGE IN CLOUD

The designed Public Auditing scheme using DHT, enhanced the privacy reservation through combining the homomorphic authenticator depending on public key with random masking generated through TPA and attained batch auditing through employing aggregate BLS signature technique. The designed scheme improved the performance of computation complexity as well as storage costs. But, the designed scheme failed to attain the secure auditing in cloud.

The designed scheme combined the Identity Based Authentication with secure quantum key distribution, to enhance the security of authentication scheme. The designed scheme employed pair of quantum bits that are entangled with each other to guarantee the security against attacks. The attack detected in real time saves the information encoded in EPR pair transmitted in authentication phase for decryption. But, quantum identity based authentication protocol leaks the information of stored files to verifier. Hence, the data integrity rate could not be enhanced by quantum identity based authentication and key agreement scheme.
Two-factor Authentication mechanism with factor revocability was used for cloud storage system. The designed system transmits the encrypted message to the receiver through the cloud storage server. The security of normal encryption scheme was not guaranteed when secret key get exposed. The security level was not improved by Two-Factor Authentication mechanism.

A. Future Direction

The future direction of the research work is to improve the security level using authentication techniques for secured data storage and transaction. In addition, the cryptographic techniques can be used to improve the authentication performance.

VI. CONCLUSION

A comparison of different existing authentication techniques for secured data storage and transaction is done. From the study, it is deduced that the existing techniques failed to improve the security performance in cloud computing. The comparative review shows data integrity rate was not improved through the quantum identity based authentication and key agreement scheme. In addition, the designed system failed to improve the efficiency, while maintaining the features. The range of experiments on existing authentication techniques for secured data storage and transaction computes the performance with its limitations. Finally, from the result, the research work can be carried out using cryptographic techniques for secured data storage and transaction with higher accuracy and minimum time consumption.

REFERENCES


