IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-8, Oct 2018 E-ISSN: 2347-2693

SURVIVAL STUDY ON DATA STORAGE AND TRANSACTION SECURITY USING AUTHENTICATION TECHNIQUES

[1*]Kavitha K, [2]Saravanan V

[1,2]Dr. NGP Arts and Science College, Hindusthan College of Arts And Science, Tamil Nadu, India

Available online at: www.ijcseonline.org

Abstract- Cloud computing is information technology (IT) model that allows the ubiquitous access to shared pools of configurable system resources and higher-level services provisioned with lesser effort. Cloud computing provides number of advantages in information technology. Cloud storage is an essential service of cloud computing that are prevalent as it present low-cost and on-demand utilization of large storage and processing resources. Security is an essential barrier to comprehensive prevalence of cloud computing. Security is mainly prioritized portion for any cloud computing environment during data storage and data transaction. Cloud computing approach is linked with users sensitive data stored both at client's end and cloud servers. For improving the security level, authentication techniques are used for allowing the authenticated user to access the data. But, complexity of the security is high when decentralization of data over the wide area of network. In addition, existing methods failed to improve the authentication accuracy and data confidentiality. Our main objective of the work is to improve the security level during the data storage and data transaction by using cryptosystem techniques.

Keywords— Cloud computing, ubiquitous, security, data confidentiality, data transaction, data storage

I. INTRODUCTION

Cloud computing is an essential element with large storage area where the resources are accessible from anyplace at anytime to everyone as a service. Cloud computing represents the high scalable computing applications, storage and platforms as service to the companies, individuals, etc. Cloud computing has formed the intangible and infrastructural source for future computing. Security is a concern for protecting the data in the cloud server. Storage security is the process of protecting the stored data from unauthorized access. Authentication is the process that guarantees and verifies the user identity. Authentication security permits only the authorized users to access and store the data in cloud. Transaction security protects the data during the transmission between two users.

This paper is organized as follows: Section 2 discusses reviews on authentication techniques for secured data storage and transaction, Section 3 explains existing authentication techniques for security enhancement, Section 4 describes the possible comparison between them, Section 5 discusses the limitations and Section 6 concludes the paper.

II. LITERATURE REVIEW

A new public auditing scheme was introduced in [1] for secured cloud storage on dynamic hash table (DHT). The designed scheme improved privacy preservation through combining the homomorphic authenticator depending on public key with random masking created through TPA. But, the designed scheme failed to achieve the secure auditing in cloud. A quantum identity based authentication and key agreement scheme was designed in [2] for cloud server architecture. A security analysis was performed using AVISPA tool for improving the security level. But, quantum identity based authentication protocol leaks information to the verifier. In addition, the data integrity rate was not enhanced using quantum identity based authentication and key agreement scheme.

Two-factor data security protection mechanism was presented in [3] with factor revocability for cloud storage. The designed system allowed the sender to transmit the encrypted message to receiver through the cloud storage server. When the device is lost, it gets cancelled and not able to decrypt any cipher text. However, the security level was not enhanced by two-factor data security protection mechanism. A new secure cloud storage system was implemented in [4] to assure the protection of data organization from the cloud provider, third party auditor and users to access the data stored on cloud. The designed system enhanced the security level through time-based one-time password and automatic blocker protocol to protect the system from the unauthorized third party auditor. But, the efficiency of designed system was not enhanced when auditing the shared data integrity.

An Extendable Access Control System with Integrity Protection (EACSIP) was carried out in [5] to enhance the

association in cloud. EACSIP was carried out in cryptographic primitive termed Functional Key Encapsulation with Equality Testing (FKE-ET). However, the integrity protection was not carried out to extend the access policy. EACSIP was not suitable for access control in collaborative situation. A light weight authentication protocol was implemented in [6] for distributed cloud where the authorized user access all information. An informal cryptanalysis authenticates that protocol is preserved against all security threats. However, the designed protocol failed to improve performance of authentication accuracy by light weight authentication protocol.

An identity-based Remote data integrity checking (ID-based RDIC) protocol was introduced in [7] with key-homomorphic cryptographic model to reduce the complexity and cost for managing public key authentication framework in PKI based RDIC methods. ID-based RDIC protocol does not leak any stored information during RDIC process. But, the authentication time was not minimized using identity-based remote data integrity checking (ID-based RDIC) protocol.

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

With fast development in network computing power and intelligent data processing capabilities, data-centric network services have extended quickly. Cloud computing is one of the original network services models in data-centric network applications for data sharing, data storage, big data organization and medical information systems. For many network services, authentication is an essential one in cloud. There are many techniques on cloud computing access authentication that concentrate on fine-grained access control servers for different users. Cloud computing are predicted as next generation of distributed computing. It is described as model for allowing suitable, on-demand network access to configurable computing resources that are provisioned and released with lesser effort.

1.Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

Cloud computing model offers feasible services like computational resources for high performance computing applications, web services, social networking, and telecommunications services. Cloud storage in data centers are useful for users to store and access data remotely at everywhere without burden. Cloud data centers have different mechanisms to denote the storage correctness and data integrity. Cloud storages in cloud data centers are employed for enterprises and individuals to store and access the data remotely without any burden. Through data outsourcing, users are mitigated from local data storage and preservation. The cloud users use the cloud storage like local storage devoid of worrying to verify the data integrity and data consistency. A third party auditor (TPA) is used in cloud computing to verify the data stored in cloud. TPA is leased by cloud service provider contract to hide the data loss from the user for preventing the defamation.

Cloud storage is a well-liked application of cloud computing that present on-demand outsourcing data services for both organizations and individuals. Users trust the cloud service providers (CSP) where it is complicated to find out whether the CSP meet their legal expectations for data security. A new public auditing scheme was designed for secure cloud storage through dynamic hash table (DHT). DHT is new two-dimensional data structure at third parity auditor (TPA) to record the information for dynamic auditing. The designed scheme transfers the authorized information from the CSP to TPA and minimizes the computational cost as well as communication overhead. The designed scheme attains higher updating efficiency. The designed scheme was used to support the privacy preservation through homomorphic authenticator depending on public key with random masking generated through TPA. The designed scheme attained batch auditing through employing the aggregate Boneh-Lynn-Shacham (BLS) signature and bilinear maps. A public auditing scheme comprises three essential functions, namely dynamic data auditing, privacy protection and batch auditing. A new data structure termed DHT collects the data properties for auditing in TPA and data updating.

2.Identity based secure authentication scheme based on quantum key distribution for cloud computing

Authentication is the process of detecting the legitimate user through validating credentials provided by user. Authentication is an essential part in successful integration of devices and cloud service provider. The key exchange scheme allocates the two parties to construct the session key. A symmetric encryption algorithm with session key attains the confidentiality between two communicating parties. Key exchange schemes without authentication are not challenging against attacks like impersonation and man-in-the-middle attack. An Authentication and Key Exchange (AKE) protocol is a key exchange scheme that built session key of two parties to maintain the secret to other parties.

Authentication is an essential one when number of hackers who seek to change into legitimate to attain sensitive information. Identity based authentication supports the identity of user where only the legitimate user gets access to the service. A quantum identity based authentication and key agreement scheme is designed for cloud server. Quantum cryptography used quantum physics laws for securing privacy and confidentiality. A formal security analysis was carried out using AVISPA tool that verifies the security.

The authentication protocols in cloud-user architecture are dependable components in network security to secure

sensitive information against malicious adversary. With fast development of computer networks, number of systems comprises a certain quantity of servers providing the service around the world. It is essential to verify the legitimate user in cloud computing environment before one is granted access to the service.

A new authentication scheme verifies the user using identity who wants to access the services of the cloud. After authentication, user accesses the cloud services. The designed scheme joined the classical identity authentication with unconditionally secure Quantum Key Distribution that improves the security level of authentication scheme. It employed an EPR pair which is the pair of quantum bits entangled with each other. The designed scheme inherits property of entanglement for improving the security. In QKD there is no chance to save information for decryption through enhanced technologies. The designed scheme minimized the opportunity window for performing the attack against QKD. The designed protocol is robust and not forged. It attained the mutual authentication and session key agreement. The designed protocol is secure against major attacks depicted using attack model.

3.Two-Factor Data Security Protection Mechanism for Cloud Storage System

A two-factor data security protection method was introduced with factor revocability for cloud storage system. The designed system assigns the sender to transmit the encrypted message to the receiver by means of cloud storage server. The sender needs to know the identity of receiver but no other information. The receiver needs two essential one to decrypt the cipher text. The first one is secret key stored in computer. The second one is unique personal security device that links to the computer. It is not possible to decrypt the cipher text without portion. When the security device is lost, device is revoked. It is not used to decrypt the cipher text. It is performed by cloud server to vary the cipher text in un-decryptable by device. The process is transparent to the sender. The cloud server failed to decrypt any cipher text at any time.

Two-factor data security protection mechanism is an Identity-based encryption mechanism (IBE). The sender needs to identify the identity of the receiver for transmitting an encrypted data and no additional information of receiver is required. The sender transmits the cipher text to cloud where the receiver download at anytime. The designed system has two-factor data encryption protection. It is not possible to decrypt the cipher text without any one of the things. When the security device is stolen or lost, device is revoked. The device failed to decrypt any cipher text in various circumstances. The user needs to utilize the new/replacement device to decrypt cipher text. The process is transparent to the sender. The cloud server failed to decrypt any cipher text at any time.

IV. COMPARISON OF AUTHENTICATION TECHNIQUES FOR SECURED DATA STORAGE AND TRANSACTION IN CLOUD & SUGGESTIONS

In order to compare the authentication techniques for secured data storage and transaction in cloud, number of cloud user requests is taken to perform the experiment. Various parameters are used for secured data storage and transaction in cloud.

1.Authentication Accuracy

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

$$Authentication\ Accuracy = \frac{Number\ of\ cloud\ user\ request\ authenticated\ correctly}{Total\ number\ of\ cloud\ user\ requests} \quad (1)$$

From (1), authenticated accuracy is calculated. When the authenticated accuracy is higher, the method is said to be more efficient.

TABLE 1 Tabulation of Authentication Accuracy

Number of cloud user requests (Number)	Authentication Accuracy (%)		
	Dynamic Hash Table-Public Auditing (DHT-PA) Scheme	Identity based Secure Authentication scheme	Two-Factor Data Security Protection Mechanism
10	78	81	69
20	80	83	71
30	82	87	73
40	85	90	76
50	81	88	73
60	79	85	70
70	83	89	74
80	85	91	76
90	87	93	79
100	89	95	82

Table 1 describes the performance of authentication accuracy with respect to number of cloud user requests ranging from 10 to 100. Authentication accuracy comparison takes place on existing Dynamic Hash Table-Public Auditing (DHT-PA)

scheme, Identity based Secure Authentication scheme and Two-Factor Data Security Protection Mechanism. From the table, it is clear that, the authentication accuracy does not get linearly increased when the number of number of cloud user requests. The graphical representation of authentication accuracy is described in figure 1.

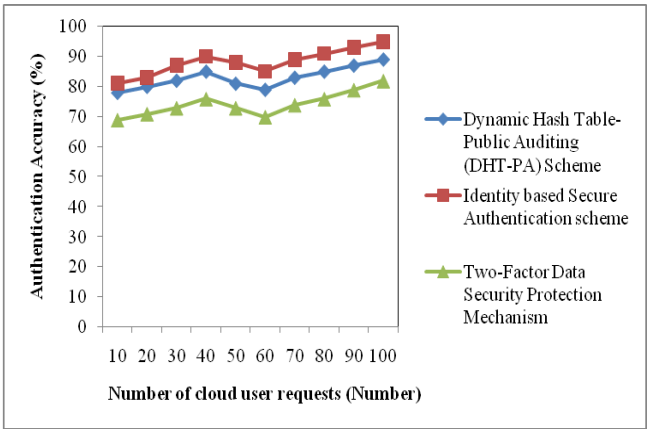

Figure 1 Measure of Authentication Accuracy

Figure 1 explains the authentication accuracy of three different techniques with respect to number of cloud user requests. Authentication accuracy of Identity based Secure Authentication scheme is comparatively higher than that of Dynamic Hash Table-Public Auditing (DHT-PA) scheme and Two-Factor Data Security Protection Mechanism. This is because the designed scheme transmits the authorized information from the CSP to TPA with minimal computational cost and communication overhead without revealing to unauthorized person with higher authentication accuracy. Research in Identity based Secure Authentication scheme consumes 6% higher authentication accuracy than Dynamic Hash Table-Public Auditing (DHT-PA) scheme and 19% higher authentication accuracy than Two-Factor Data Security Protection Mechanism.

2.Authentication Time

Authentication time is defined as the amount of time consumed for performing the authentication process. Authentication Time is defined as difference of staring time and ending time of authentication. It is measured in terms of milliseconds (ms) and given by,

$$Authentication\ time = Ending\ time - starting\ time\ of\ authentication$$

$$Authentication\ time = Ending\ time - starting\ time\ of\ authentication$$

Authentication time =
Ending time – starting time of authentication

(2)

From (2), authenticated time is determined. When the authentication time is lesser, the method is said to be more efficient.

TABLE 2 Tabulation of Authentication Time

Number of cloud user requests (Number)	Authentication Time (ms)		
	Dynamic Hash Table-Public Auditing (DHT-PA) Scheme	Identity based Secure Authentication scheme	Two-Factor Data Security Protection Mechanism
10	23	35	42
20	26	37	45
30	22	34	41
40	25	36	46
50	28	40	50
60	24	38	47
70	27	42	53
80	25	37	49
90	29	40	54
100	31	44	58

Table 2 explains the performance of authentication time with respect to number of cloud user requests ranging from 10 to 100. Authentication time comparison takes place on existing Dynamic Hash Table-Public Auditing (DHT-PA) scheme, Identity based Secure Authentication scheme and Two-Factor Data Security Protection Mechanism. From the table, it is clear that, the authentication time gets changed when the number of number of cloud user requests varied. The graphical representation of authentication time is explained in figure 2.

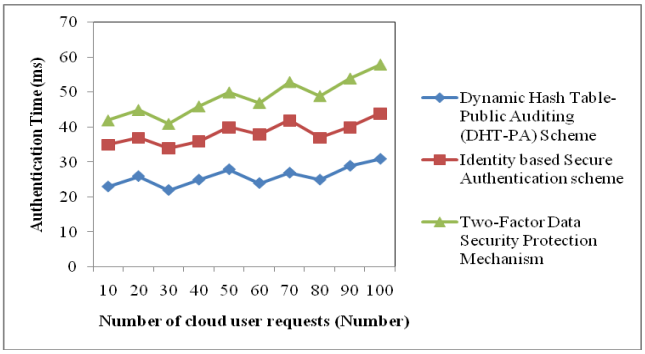

Figure 2 Measure of Authentication Time

Figure 2 illustrates the authentication time of three different techniques with respect to number of cloud user requests. Authentication time of Dynamic Hash Table-Public Auditing

(DHT-PA) scheme is comparatively lesser than that of Two-Factor Data Security Protection Mechanism and Identity based Secure Authentication scheme. This is because the designed scheme joined the classical identity authentication with unconditionally secure Quantum Key Distribution which enhances the security level of authentication scheme with minimal time consumption. Research in Dynamic Hash Table-Public Auditing (DHT-PA) scheme consumes 32% lesser time for authentication than Identity based Secure Authentication scheme and 46% lesser time for authentication than Two-Factor Data Security Protection Mechanism.

3.Data Confidentiality Rate

Data confidentiality rate is defined as rate at which the data gets transacted to an exact user without unauthorized access. Data Confidentiality rate is the measure of ability of system to protect their data. The confidentiality explains the authorization checks to guarantee the blocks that are not accessed by the entities without any rights. It is measured in terms of percentage (%).When the data confidentiality rate is higher, the method is said to be more efficient.

TABLE 3 Tabulation of Data Confidentiality Rate

Number of cloud user requests (Number)	Data Confidentiality Rate (%)		
	Dynamic Hash Table-Public Auditing (DHT-PA) Scheme	Identity based Secure Authentication scheme	Two-Factor Data Security Protection Mechanism
10	65	72	81
20	67	74	83
30	69	78	85
40	72	80	87
50	68	75	84
60	73	79	88
70	76	82	90
80	74	80	86
90	77	85	88
100	83	88	92

Table 3 illustrates performance of data confidentiality rate with respect to number of cloud user requests ranging from 10 to 100. Data confidentiality rate comparison takes place on existing Dynamic Hash Table-Public Auditing (DHT-PA) scheme, Identity based Secure Authentication scheme and Two-Factor Data Security Protection Mechanism. From the table, it is clear that, the data confidentiality rate does not get linearly increased when the number of cloud user requests gets increased. The graphical representation of data confidentiality rate is explained in figure 2.

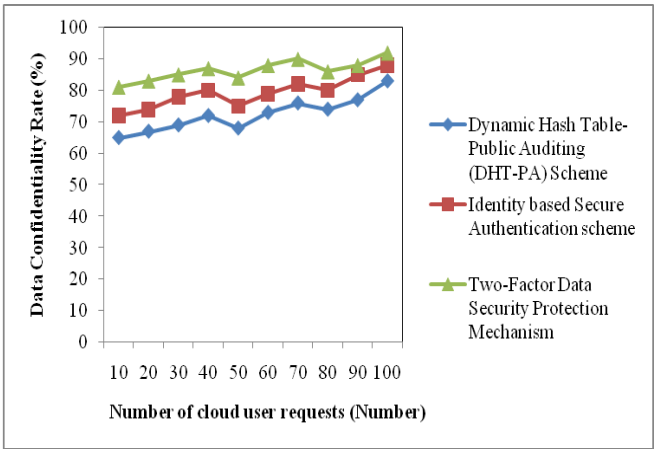

Figure 3 Measure of Data Confidentiality Rate

Figure 3 portrays data confidentiality rate of three different techniques with respect to number of cloud user requests. Data confidentiality rate of Two-Factor Data Security Protection Mechanism is comparatively higher than that of Dynamic Hash Table-Public Auditing (DHT-PA) scheme and Identity based Secure Authentication scheme. This is because of using Identity-based encryption mechanism (IBE). In this designed mechanism, the sender identifies receiver identity for transmitting encrypted data. The sender transmits the cipher text to the cloud where the receiver download data at anytime with higher data confidentiality rate. Research in Two-Factor Data Security Protection Mechanism has 20% higher data confidentiality rate than Dynamic Hash Table-Public Auditing (DHT-PA) scheme and 9% higher data confidentiality than Identity based Secure Authentication scheme.

V. DISCUSSION ON LIMITATION OF AUTHENTICATION TECHNIQUES FOR SECURED DATA STORAGE AND TRANSACTION IN CLOUD

The designed public auditing scheme enhanced the privacy preservation 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 attained secure auditing in clouds and improved performance of computation complexity as well as storage costs. However, the designed scheme failed to attain the secure auditing in cloud. The designed scheme combined the identity 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 save 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. The data integrity rate was not enhanced by quantum identity based authentication and key agreement scheme.

Two-factor data security protection 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 data security protection mechanism.

1.Related Works

A comparative analysis of cryptographic defence technique was carried out in [8] and addressed the outsource data protection in cloud infrastructures. But, the processing complexity was not minimized and considered as an essential requirement for security. In addition, privacy-preserving ability at secured broadcast channels was impractical and burdensome to implement. A new fine-grained two-factor authentication (2FA) access control system was implemented in [9] for web-based cloud computing services. An attribute-based control allowed the cloud server to limit the access to users with set of attributes while protecting the user privacy. A perception behind proof server failed to differentiate the attributes used by cloud users in authentication process. In addition, the designed system failed to improve the efficiency while maintaining the features.

Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE) was used in [10] for key management, access control and file deletion. Multiple key managers removed the single point of failure for cryptographic keys. DaSCE methodology was not extended to the secure group shared data and secured data forwarding.

2.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 studied. From the study, it is observed that the existing techniques failed to improve the security performance in cloud computing. The survival 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 wide 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 lesser time consumption.

REFERENCES

[1] Hui Tian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen and Jin Liu "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", IEEE Transactions on Services Computing, Volume 10, Issue 5, September-October 2017, Pages 701 – 714

[2] Geeta Sharma and Sheetal Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing", Peer-to-Peer Networking and Applications, Springer, Volume 11, Issue 2, March 2018, Pages 220–234

[3] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu and Yang Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, Volume 65, Issue 6, June 2016, Pages 1992 – 2004

[4] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", EURASIP Journal on Information Security, Springer, Volume 13, December 2016, Pages 1-13

[5] Willy Susilo, Peng Jiang, Fuchun Guo, Guomin Yang, Yong Yu and Yi Mu, "EACSIP: Extendable Access Control System with Integrity Protection for Enhancing Collaboration in the Cloud", IEEE Transactions on Information Forensics and Security, Volume 12, Issue 12, December 2017, Pages 3110 – 3122

[6] Ruhul Amin, Neeraj Kumar, G.P. Biswas, R. Iqbal and Victor Chang, "A Light Weight Authentication Protocol for IoT-enabled Devices in Distributed Cloud Computing Environment", Future Generation Computer Systems, Elsevier, Volume 78, Part 3, January 2018, Pages 1005-1019

[7] Yong Yu, Man Ho Au Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information Forensics and Security, Volume 12, Issue 4, April 2017, Pages 767 – 778

[8] Nesrine Kaaniche and Maryline Laurent, "Data Security and Privacy preservation in Cloud Storage Environments based on Cryptographic Mechanisms", Computer Communications, Elsevier, Volume 111, 1 October 2017, Pages 120-141

[9] Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu and Jin Li, "Fine-grained Two-factor Access Control for Web-based Cloud Computing Services", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 3, March 2016, Pages 484 – 497

[10] Mazhar Ali, Saif U. R. Malik and Samee U. Khan, "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transactions on Cloud Computing, Volume 5, Issue 4, October-December 2017, Pages 642 – 655

