EXCELLENT PUBLISHERS

International Journal of Current Research and Academic Review

ISSN: 2347-3215 (Online) Volume 9 Number 01 (January-2021)

Journal homepage: http://www.ijcrar.com

doi: https://doi.org/10.20546/ijcrar.2021.901.011

A Dual Authentication Mechanism for Cloud Computing to Provides Security in Cloud Data Storage

Gulfishan Firdose Ahmed[1]* and Raju Barskar[2]

[1] *Department of Computer Science, College of Agriculture, JNKVV, Powarkheda, Narmdapuram, India*
[2] *Department of Computer Science and Engineering, University Institute of Technology, RGPV, Bhopal, India*

**Corresponding author*

Abstract

The popular trend in today's technology driven world is ‘Cloud Computing’. Cloud computing has become the growing idea in the sector of IT. Cloud computing helps the user to store and access their data over the internet rather than their computer's hard drive. Cloud Computing addresses that data is stored at a local place and is synchronized with other web information over the network. In today’s world, cloud computing is used at many places including small or big business. As it includes wide range of data and people, therefore there is a requirement to make it protected. Cloud security is the one way of protecting the data using many encryption and decryption techniques. Again, there requires the need of authentication. Authentication is the process by which we can know whether a user is authenticated or not. There are certain authentication techniques, which are used for the authentication of the users. Here proposed, a dual authentication technique, which consists of three phases, which provide high data security to the cloud storage. The uses of authentication techniques are makes our data safe and secure.

Article Info

Accepted: 08 December 2020
Available Online: 20 January 2021

Keywords

Cloud Computing, Cloud Storage, Cloud Security, Authentication, Data Security Model.

Introduction

Cloud Computing is changing our lives day by day. All the day to day activities like banking, E-mail, Media, Streaming, and Ecommerce all use the Cloud. Cloud Computing offers services and applications that are offered on numerous devices over worldwide. Cloud Computing is not just used by the organizations, but also it is useful for average people as it does not require any installation on our system.

It only requires good quality of internet and all the services could be accessed as pay per use. These offerings are provided over three different types of cloud. Cloud security is the safeguarding of data stored on the cloud services online provided by the cloud service providers. The data can be interrupted by malicious user who may change the data. Authentication is the mechanism of identifying whether someone or something is who or what it declares to be. Authentication technology provides access control for the systems to check if a user’s credentials match the credentials in the database of authorized users or the authorized network.

Users are provided with user ID, and authentication is accomplished when the user provides his/her credentials, for example the password matches with the password stored in the database. There can be a single authentication factor or multifactor authentication.

Authentication is one of the techniques who play a major role in cloud data security. The various possible security attacks on the CSP (Cloud Service Provider) are prevented by applying different authentication techniques, which verifies whether a user is authenticated or not by identity when a user wishes to request the services from the cloud service providers. It prevents the shared information from the outsiders i.e. the users who are not authorized. This proves the user is authenticated and can access further.

Literature Survey

In (1) this paper reviews that authentication is one of the major techniques in cloud computing security. In this paper he explains various methods of authentication., as authentication plays a marvellous role in maintaining the validation of the shared data in cloud, thereby increasing the security which is the major issue in cloud computing environment. This shows their paper (2) identifies that the issues related to cloud computing deployment are security, attacks, privacy and trust which reduces its use and benefit to user.

This paper also suggests that the most popular Identity Management System (Idm), working in the field of mobile cloud has many faults in authorization architecture. In this paper they indicated some limitations into their access control model, like that of stealing the access tokens during authorization.

As a solution, they proposed some modifications to the original access control model. They (3) proposed a model which allows users to authenticate to the service securely and control the disclosures of their attributes.

Their model produces the user a flexibility to make instant identity along with credential required to authenticate service provider. In this approach, there are multiple adhoc identities for users that can be used during supply of personal credentials to the service provider. Paper shows (4) privacy-preserving authentication protocol for efficient data security was proposed. New challenges to privacy can be brought by users who want to access and share each other's authorized data fields to achieve dynamic benefits from the cloud.

An efficient attribute based access control is adopted to understand that the user can only provide data sharing among different users. It is focus on applications where the inaction of the computation should be reduced, i.e. the computation should be as small as possible for submitting the query until receiving the outcomes(5). Proposed (6) a hybrid algorithm which uses encryption as a primary security policy. Encryption is a process which translates data into another form i.e. from plain text to cipher text, so that only people who can access through the secret key can read it. In today's world, encryption is the most popular and effective for data security.

The proposed hybrid algorithm comprises of different encryption –decryption techniques such as AES (symmetric cryptography technique), SHA-1(hashing technique), and ECC (elliptic curve cryptography) for the categorized sensitive data. During transit as well as storing, there is a main aim of this algorithm to increase the data owner's control of data.

A three-tier privacy aware cloud computing model is proposed for three categories of the data, NP, PTP, and PNTP. In (7) along with his colleagues, evaluated the existing model of data duplication in cloud computing. Some of the cloud storage techniques like chunk calculation, distributed hash table and bloom filter has contributed to load balancing management in cloud computing systems.

They identified several risks associated with cloud computing such as Data access, Lack of trust and authentication, Data Segregation, Data Breaching, Virtual Machine Security, VM Sprocol, Verification of Identity and signatures.

Proposed Work

To reduce the problem of unauthorized access, we have designed a dual authentication technique for secure data transmission in cloud data storage.

Explanation of the Method Using A Flowchart

This is the entire mechanism used in the dual authentication technique. It consists of three phases which are described in the flowchart given below. Here a mechanism is designed which consists of three phases such as:-

1) **Registration Phase** –In this phase, the user registers to the cloud services through his various credentials like e-mail id, mobile number and password to the CSP. After the completion of registration, the CSP provides USK_i to the registered candidate which is unique for every user

2) **Authentication Phase** –In this phase, the user and the CSP authenticates each other by providing hash code and encrypting it and again decrypting it to get the authenticated code back. If both the hash codes match with each other, then the user is authenticated. If they do not match the user is unauthorized and he is not allowed to access the services of the cloud.

3) **Access Service Phase-** In this phase, if the user is authenticated he can access the services of the cloud. The user is allowed to access the services using the session key. The user and the cloud create the session key using the Diffie-Hellman key exchange. If both session keys are matched then their services are enabled.

This procedure is highly secure as it creates dual authentication and the role of any attacks or intruder attack is prevented. The user, CSP, and the cloud server creates a highly secure transmission network and then the user can store his data in the cloud storage.

Details of Algorithms

(i) SHA-256 – During the authentication request phase, the CSP generates the HC using the random number N and the USK by SHA_256 algorithm and then verifies the newly computed HC value with the HC which is sent from the user side. If the two HC value match, then the CSP hashes the Hash Code to get the Authentication Code (AC).

(ii) Diffie-Hellman Key exchange – User and Cloud have setup their session key for the access service phase. First the user asks cloud for the transmission of data with Diffie-Hellman parameter, and then the cloud gives back the response to the cloud. After this the session key is generated. Now the transmit message can be encrypted. Now also transmit the encrypted message with code.

Method Using Dual Authentication and its Results

In this technique, the user and the cloud service provider are authenticated by each other, so that no unauthorized user can access the data stored by the user in the cloud server. Here, the entire process which includes three phases is explained below with the description of every phase and their requirements. The notations are explained in the table provided below, these notations are used in the proposed technique (11-17).

Phase :I– User Registration Phase

(i) Foremost of all the services of cloud storage to be accessed by the user, the users have to register with the Cloud service provider. The user is required to enter all the credentials, which are important for the registration process. The credentials like his username, password and e-mail id. The entered details are stored on the CSP end.

(ii) While each user performs registration, the CSP provides a unique code to the user, which later is used at the time of authentication of the users.

(iii) After the completion of the registration process, the CSP provides the USK_i to the registered candidates. Which is unique for every user and the CSP also maintains the list of all the registered users and their respective USK_s in the storage area. The CSP provides the USK_i to the users through e-mail, and the generated code on their mobile number.

Phase 2 – User's Authentication Process

User store (USK_i) with them. Then he first enter his /her code through the option apply code. Then the cloud server compares the cloud with the code stored in the database. If they match the user is allowed for the access of services in cloud.

Phase3--Cloud Service Provider's Authentication Process and the Provision of Authenticated code (AC)

User selects random number N.

$$HC = SHA - 256(USK \parallel N) \ldots (1)$$

This is the Authentication Request-

$$\langle EUSK(N \parallel HC \parallel IDU) \parallel (IDU \parallel IDCSP \parallel TS1)\rangle \ldots (2)$$

Then the CSP chooses two numbers – a_1 and b_1 such that

$$a_{1,} b_1 \in Z_q^*$$

And identity of user is calculated by using $IDU = g_1^{a_1} \times g_2^{b_1} \mathrm{mod} q$ Here, g_1 and g_2 are the generators of Z_q^*

Cloud server receives the packet, appends its identity ID_{CS} and increments timestamp value TS_1 to get TS_2.Then the Cloud server encrypts the entire message using the CSK which is known only to Cloud service provider and cloud server as given in the Equation below-

$$\langle E_{CSK}(E_{USK}(N \parallel HC \parallel ID_U) \parallel ID_U \parallel ID_{CSP} \parallel TS_2 \parallel ID_{CS})\rangle \ldots (3)$$

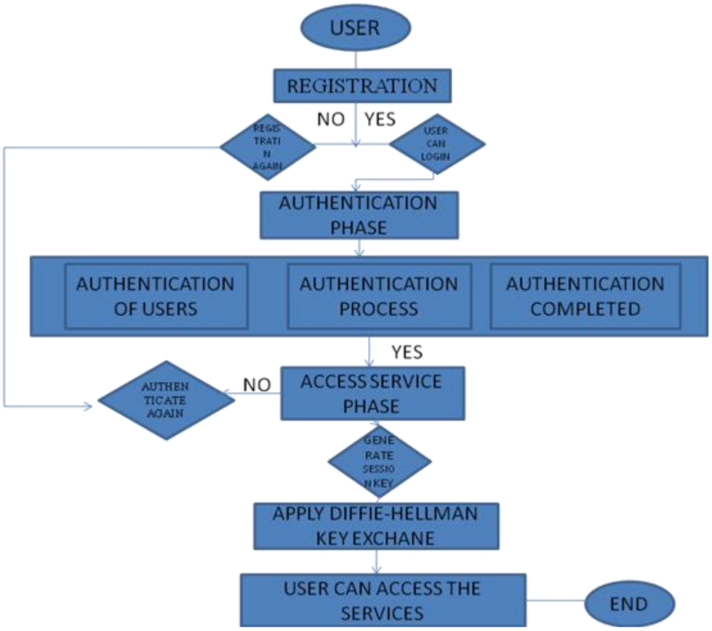
The Cloud service provider decrypts the packet received from CS using CSK of the CS and validates the CSK with its identity ID_{CSK} as given in Equation (4).

$$\langle D_{CSK}(E_{CSK}(E_{USK}(N \parallel HC \parallel ID_U) \parallel ID_U \parallel ID_{CSP} \parallel TS_2 \parallel ID_{CS}))\rangle \dots (4)$$

The cloud service provider also verifies its identity ID_{CSP} after decrypting it using CSK. After verifying its identity, the CSP decrypts the packet using USK of the particular user and verifies the $ID_{U.}$

$$\langle D_{USK}(E_{USK}(N \parallel HC \parallel ID_U))\rangle \dots (5)$$

Figure.1 Proposed Dual Authentication Mechanism



Then, the CSP generates the HC using this random number N and the USK by SHA_256 algorithm and then verifies the newly computed HC value with the HC which is sent from the user side. If the two HC value match, then the CSP hashes the Hash Code to get the Authentication Code (AC)

$$AC = SHA_{256(HC)} \dots (6)$$

The CSP includes the user ID, incremented time stamp value and also it includes the lifetime of the AC along with the AC and encrypts this sequence with its private key of CSP (CSP- Pvt) to create a digital signature.

Thus any of the user can verify their digital signature using the public key of CSP. But, no user can regenerate this digital signature because it is generated using the private key of the CSP.

$$\langle E_{CSP-Pvt}(AC \parallel ID_U \parallel TS_3 \parallel Lifetime)\rangle \dots (7)$$

This forms the authentication response. To securely transfer this AC to the correct user, the Cloud service provider also encrypts this authentication response using the USK value of the corresponding user and CSK of Cloud server.

$$\langle (E_{CS}(E_{USK}(E_{CSP-Pvt}(AC \parallel ID_U \parallel TS_3 \parallel Lifetime))) \parallel ID_{CSP})\rangle \dots (8)$$

Finally, the cloud service provider sends the packet to cloud server. Cloud server receives the packet from CSP and decrypts the packet using its CSK.

$$\langle D_{CS}(E_{CS}(E_{USK}(E_{CSP-Pvt}(AC \parallel ID_U \parallel TS_3 \parallel Lifetime))) \parallel ID_{CSP})\rangle \dots (9)$$

On receiving this message, the cloud server is able to check the identity of cloud service provider (ID_{CSP}), verifies that whether it is sent by the legitimate cloud service provider or any malicious node. After verifying the identity of CSP, the cloud server sends the packet to the user.

$$\langle E_{USK}(E_{CSP-Pvt}(AC \parallel ID_U \parallel TS_3 \parallel Lifetime))) \parallel ID_{CSP})\rangle \ldots (10)$$

The user decrypts the packet using its USK, and then verifies ID_{CSP},

$$\langle D_{USK}\langle E_{USK}(E_{CSP-Pvt}(AC \square ID_U \square TS_3 \square Lifetime))) \square ID_{CSP})\rangle -------(11)$$

After that, the user verifies the ID_U by decrypting the resultant message using the public key of the Cloud service provider.

$$\langle D_{CSP-Pub}(E_{CSP-Pvt}(AC \square ID_U \square TS_3 \square Lifetime))\rangle --(12)$$

Phase Three-- Access Service Phase

Suppose user want to communicate with the cloud i.e. access the services of the CSP.

User selects his/her private key P_U.Then the user calculates his public key and sends to the cloud. Cloud selects its private key P_C. Then it calculates its public key and sends to user. Once the user receives cloud's public key, he can generate the session key(20-22):

$(Pri_C)^{Pub}{}_U$ meanwhile cloud can calculate its session key: $(Pri_U)^{Pub}{}_C$ once he receives user's public key.

Set up the session key- User→ Cloud: Message (ask cloud for the transmission of data with Diffie-Hellman parameter a, q, Pri_U**) *Code$_U$ (M$_1$|TS),Cert$_{user}$***

Cloud →User:M_2 (respond with Diffie Hellman parameter Private $_{cloud}$) ***Code$_{cloud}$ (M$_2$|TS),Cert$_{cloud}$, HMAC$_{SK}$(M$_2$)***

User→Cloud: M_3 (session key is built), ***HMAC$_{SK}$(M$_3$)***

Transmit subsequent encrypted message ***User→Cloud: E$_{sk}$ (m)***

Transmit subsequent encrypted message with code-***User→Cloud: E$_{sk}$ (m|Code(HMAC$_{SK}$(m)))***

On the setup of the session key, user defines a primitive root of a prime number q. Then the user select a random number P_u and computes $Private_U=a^{PU}modp$. The cloud and the user can thus communicate with each other. The user can further access the services of the cloud (22-28).

Future Work

Due to the wide usage of cloud platform for various applications over a few years, users concern about maintaining his privacy of the data becomes vital. In cloud computing, security plays a vital role in cloud data storage and data transmission that needs to be addressed. Therefore the growth of rust has become the main motivation of this research. Out of different techniques which are used for cloud security, authentication is one of the main factors to be secured. Actually, authentication of user becomes an important issue in cloud computing in order to protect the personal information in cloud service providers. There are many authentication techniques which are used as a medium for enhancing the security which works as the main loophole or issue in cloud computing. The various authentication techniques help the user to store their data or application on Untrusted Cloud environment. In the future several other methods can be used for the authentication of the user. The use of cloud security techniques will be increased and various cryptographic and authentication methods can be implemented for high security results. In our method, we can also add more security parameters for better results. Hence, the user risk of data loss can be improved.

References

1. Ahmad, A., Hassan, M. M., & Aziz, A., "A multi-token authorization strategy for secure mobile cloud computing", In *2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, pp. 136-141, April 2014.
2. Baghele, K., Barskar, R., & Chourasia, U., "Adoption of Green Cloud Computing—A Review", In *Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 1* (pp. 915-925). Singapore: Springer Nature Singapore,
3. Behl, A and K Behl, "An analysis of cloud computing security issues", IEEE,2012.
4. Dewangan, B. K., Agarwal, A., & Pasricha, A. (2016, October). Credential and security issues of cloud service models. In *2016 2nd International*

Conference on Next Generation Computing Technologies (NGCT) (pp. 888-892). IEEE.

5. Divya, S. V., Dr. Shaji R. S., ”Security in data forwarding through elliptic curve cryptography in cloud”, IEEE, pp. 1083–1088, 2014.
6. Farooq, H., “A Review on cloud computing security using authentication techniques”, *International Journal of Advanced Research in Computer Science*, *8*(2), 2017.
7. Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010, September). The characteristics of cloud computing. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 275-279). IEEE.
8. Goyal, V., & Kant, C. (2018). An effective hybrid encryption algorithm for ensuring cloud data security. In *Big Data Analytics: Proceedings of CSI 2015* (pp. 195-210). Springer.
9. Iyer, K. P., Manisha, R., Subhashree, R., & Vedhavalli, K. (2016, February). Analysis of data security in Cloud Computing. In *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)* (pp. 540-543). IEEE.
10. Jain, P., Barskar, R., & Chourasia, U. (2022, November). Attacks and Security Schemes in Cloud Computing: A Survey. In *Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 1* (pp. 859-874). Springer.
11. Jain, P., Barskar, R., & Chourasia, U., “Attacks and Security Schemes in Cloud Computing: A Survey”, In *Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 1* (pp. 859-874). Singapore: Springer Nature Singapore, November, 2022.
12. Jain, P., Chourasia, U., & Barskar, R. (2022, March). IP based Dual Data Security for Cloud Storage Against Denial-of-Service Attack. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1228, No. 1, p. 012018). IOP Publishing.
13. Jaiswal, S., Ahirwar, M., & Baraskar, R. (2017). Intruder Notification System & Security in Cloud Computing: A Review.
14. Kumar, S., Shekhar, J., & Singh, J. P. (2018). Data security and encryption technique for cloud storage. In *Cyber Security: Proceedings of CSI 2015* (pp. 193-199). Springer Singapore.
15. Manimaran, A., & Somasundaram, K., “An Efficient Data Security Mechanism in Cloud Computing Using Anonymous ID Algorithm”.
16. Muthulakshmi, B., & Venkatesulu, M. (2017). Cloud Data Security Based on Data Partitions and Multiple Encryptions. In *Theoretical Computer Science and Discrete Mathematics: First International Conference, ICTCSDM 2016, Krishnankoil, India, December 19-21, 2016, Revised Selected Papers 1* (pp. 191-196). Springer International Publishing.
17. Muthulakshmi, B., & Venkatesulu, M. (2017). Cloud Data Security Based on Data Partitions and Multiple Encryptions. In *Theoretical Computer Science and Discrete Mathematics: First International Conference, ICTCSDM 2016, Krishnankoil, India, December 19-21, 2016, Revised Selected Papers 1* (pp. 191-196). Springer International Publishing.
18. Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580.
19. Prajapati, K. S., Chourasia, U., Baraskar, R., & Dixit, P. (2021). Privacy and Security Issues in Fog Computing. *Solid State Technology*, *64*(2), 1331-1339.
20. Qian, L., Luo, Z., Du, Y., & Guo, L. (2009). Cloud computing: An overview. In *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1* (pp. 626-631). Springer Berlin Heidelberg.
21. Rizvi, S., Ryoo, J., Kissell, J., Aiken, W., & Liu, Y. (2018). A security evaluation framework for cloud security auditing. *The Journal of Supercomputing*, *74*, 5774-5796.
22. Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, *86*(9), 2263-2268
23. Soni, D., & Patel, H., “Privacy preservation using novel identity management scheme in cloud computing”, In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pp. 714-719, April 2015.
24. Srivastava, P and R Khan, “A Review Paper on Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume-8, 2018.
25. Suhui, G., Quan, W., & Wenhui, S. (2018). Security Strategy of Campus Network Data Center in Cloud Environment. In *Cloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8–10, 2018, Revised Selected Papers, Part III 4* (pp. 290-297). Springer International Publishing.
26. Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing.

International Journal of Distributed Sensor Networks, *10*(7), 190903.

27. Tripathi, A., & Mishra, A. (2011, September). Cloud computing security considerations. In *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)* (pp. 1-5). IEEE.
28. Tyagi, M., Manoria, M., & Mishra, B. (2019). Effective data storage security with efficient computing in cloud. In *Communication, Networks and Computing: First International Conference, Gwalior, India, March 22-24, 2018*, (pp. 153-164). Springer
29. Wei, Y., & Zhang, Y. (2018). Cloud computing data security protection strategy. In *Cloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part I 4* (pp. 376-386). Springer International Publishing.
30. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

How to cite this article:

Gulfishan Firdose Ahmed and Raju Barskar. 2021. A Dual Authentication Mechanism for Cloud Computing to Provides Security in Cloud Data Storage. *Int.J.Curr.Res.Aca.Rev.* 9(01), 126-132.
doi: https://doi.org/10.20546/ijcrar.2021.901.011