DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4566

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

MULTI-FACTOR AUTHENTICATION USING A NOVEL APPROACH IN THE CLOUD

S.Meena
Research Scholar,
Department of Computer Science,
Periyar University,
Salem-11,India

Dr.V.Gayathri
Asst.Professor
Department of Computer Science,
Peegee College of Arts and Science,
Periyanahalli- 635 205,India

Abstract: Cloud computing is a contemporary prototype to deliver services over the Internet. Cloud security is the most crucial issue in a cloud atmosphere either it is public cloud or community cloud. There is a vast scope to scrutinize data security enhancement in cloud storage. Authentication is an essential technology for information security, which is a mechanism to confirm proof of identities to obtain access of information in the system. Conventionally used authentication methods are rather securing data, but not smart enough and completely secured. In this paper, we have implemented a novel verification technique that associate with static username and password as a way in authentication followed by OTP based on the token generator method along with a digital signature and image captcha is an innovative factor to verify an each user. The solution aims at gaining confidentiality and integrity by making use of CP-ABHE (Ciphertext Policy-Attribute based Homomorphic Encryption algorithm) and user verification with Multi-Factor Authentication. Finally the efficiency of the system is examined with the help of the experimental results and discussions.

Keywords: Public cloud, OTP, Image captcha, Digital Signature, CP-ABHE, Confidentiality.

1. INTRODUCTION

In the developing technologies cloud computing placed a crucial role in various applications such as education, research, banking and other important sectors [1]. These applications requires lot of information for making effective process, for this purpose, cloud provides the enormous amount of on demand services such as monitoring services, finance applications, database with affordable cost [2]. During the service providing process, cloud computing technology consists of different characteristics namely on demand services, resource pooling, elasticity, Productivity, Reliability, Scalability, Security and Agility. By using the different characteristics cloud provides the services [3] in terms of platform as services (PaaS), infrastructure as services (IaaS) and software as a services (SaaS). Even though the cloud provides the effective services, security is one of the important challenges due to intermediate attacks and unauthorized access [4]. 70% of industries reported that the security is one of the main challenges while sharing and accessing the data in the cloud because it has followed particular set policies, controls, technologies [5]. These security mechanisms have been hacked by intermediate attacks that will lead to create the untrust between cloud service provider and cloud service requestor because the service requestor initially registered their personal details before accessing services [6]. The personal information may contains any sensitive information such user name, password, banking details, phone number etc. These sensitive information may be accessed and misused by third party which may create the untrust between both parties [7].This security issues is handled by applying the different cryptographic algorithms such as both symmetric and asymmetric techniques [8] such as Advance Encryption Standards (AES), data encryption standards (DES), blowfish, two fish, RSA, MD5, SHA, key policy based encryption methods, attribute based encryption, public key encryption methods and so on. These encryption algorithms manage the user registered information by performing the encryption and decryption process to avoiding the intermediated access [9]. Before performing the cryptographic process, user need to register their details by signup the particular cloud service page using user name, password and other personal details which is encrypted by cloud provider and that is stored in the cloud server. After that user need to sign in that page using user name and password then the cloud provider sent the one time password (OTP) [10] to the user mobile phone. Based on the received OTP, user again login to the particular page, the cloud provider compares the details with the encrypted cipher text for providing the cloud services to the user. Even though the traditional encryption methods successfully maintains the security between the service provider and requestor, the private key and user details are hacked by intermediate attacks which leads to create security problem again. So, in this paper introduces the Ciphertext policy attribute [11] based homomorphic encryption algorithm along with the digital signature process. The introduced method uses the static username and password for authentication purpose by using the OTP based token generator [12]. Along with the normal authentication process, the method utilizes the image captcha process for user verification process. Thus the introduced multi factor authentication process ensures the security and trust between the provider and requestor with effective manner. Then the efficiency of the system is evaluated with the help of the cloudsim tool based experimental analysis.

Then the rest of the paper is organized as follows, section 2 analyze different researches works based on the security

issues in cloud. Section 3 discusses the proposed cipher text policy attribute based homomorphic encryption algorithm along with the digital signature process. Section 4 examines the proposed systems experimental results and concludes in section 5.

2. RELATED WORKS

In this section analyze the various researches opinions about the cloud security issues. Shobha Rajak et al.,[13] analyzing the protection issues present in the cloud environment because the cloud services are used in different purposes such as storage, auditing, requirement collection of different bench data. Among the different characteristics, author ensures the cloud security by using the digital signature process. Based on the digital signature process, service provider manages the data center, data privacy by encrypting the user signature with the help of the RSA encryption algorithm. Then the performance of the system is evaluated by utilizing cloudsim implementation tool. Thus the author developed system successfully provides the security to the user sensitive data.

Shivam Patole et al.,[14] examining the data confidentiality and data privacy in the cloud using the key policy attribute based encryption method. This encryption process work according to the homomorphic encryption process that effectively manages the key while encrypting the user details with effective manner. Further the author implements the client based confidentiality tools for overcoming the security issues. The efficiency of the system is evaluated with the help of the experimental results, thus the system ensures the security with minimum encryption time and minimum cost.

Prachi Soni**,** et al., [15] proposing the multi factor authentication framework for implementing the data security in cloud environment. The developed multi factor system analyzes the different features such as confidentiality, integrity, privacy and authentication while providing the services to the user. The author establishes the security via the zero knowledge proof protocol which successfully encrypts the user information in the cloud service provider side. The efficiency of the system is evaluated using the experimental results. Based on the above discussions, the cloud security is established by using the multi factor authentication process. So, in this paper introduces the cipher text policy attribute based homomorphic encryption algorithm which ensures the security by using three different stages. During the encryption process the author uses the digital signature along with image captcha for establishing the efficient security in the cloud environment. The rest of the section discuss the proposed security establishment process.

3. Proposed cipher text policy attribute based homomorphic encryption algorithm along with the digital signature process

In this section discusses about the proposed cipher text policy attribute based homomorphic encryption algorithm along with the digital signature process for ensuring the security while accessing services in cloud. The detailed working structure of the proposed system is shown in the figure 1.

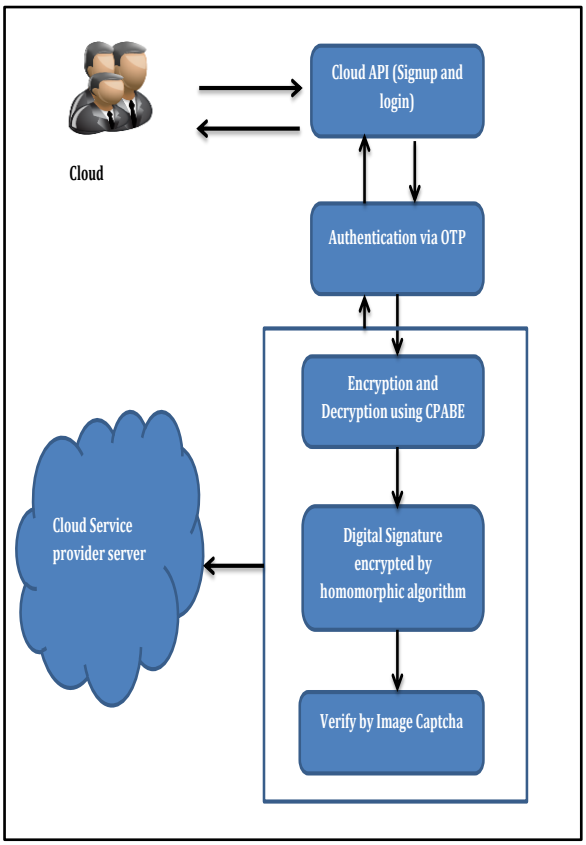

Figure 1: Proposed CPABE Homomorphic based Cloud security architecture

The above figure 1 clearly depicted that the proposed cloud security architecture which consists of three stages of verification process namely normal user personal information encryption and decryption process, digital signature encryption process and finally image captcha verification. This three stage encryption process gives more security to user sensitive details also eliminates intermediate attack with efficient manner. The detailed explanation of the proposed CP-ABE homomorphic cloud security process is explained as follows.

3.1 Stage 1

Initially the cloud users request the cloud provider for accessing the particular cloud service by signup their personal information. During the registration process, the user enter their name, phone number, email id and so on, these details are need to maintain confidentially because the unauthorized user may be access those information which leads to create serious problem in future [16]. By entering the user details, the cloud service provider generates the one time password (OTP) and sends these message to user entered phone number. After that user need to enter the OTP number to respective column. Based on the initial verification process, the user entered personal information is saved confidentially by performing the encryption process which is done by applying the Cipher text Policy-Attribute based encryption method [17].This algorithm only encrypts the user sensitive data expect the digital signature by

usingfour steps such as setup, encryption, key generation and decryption which is explained as follows,

Setup (a, U)

The first step input parameters setup, in which the security parameter and attribute universe parameter has been initialized as the input. Also generates the public parameters pk and master key mk.

Key Generation (Mk, s)

The second step is key generation in which the set of attributes relative keys are need to be generated. Sk means decryption key which is used only for the decryption purposed at the time ser verification process. The decryption process is done by as follows,

$$sk = cpabe\_keygen\ (group, mk, pk, attributes)$$

Encrypt (pk, m, A)

The encryption process encrypts the message m by using the structure attributes and public key and generates the cipher text C.

$$sessionkey = decryptsessionkey(sctxt, mk, pk, attributes)$$
$$ciphertext = encrypt\ \{(plaintext, pk), sessionkey\}$$

In this encryption process, the session key is the random value that is generated by the user whereas, it is the combination of the session key and access policy.

Decrypt (pk,ct,sk)

The last step is decryption which is done by using the cipher text (ct), private key and set of attributes which is defined as follows,

$$sessionkey = decryptsessionkey\ (sctxt, pk, sk, attributes)$$
$$dec = decrypt(ciphertext, pl, sk, sessionkey)$$

These four steps are performed successfully while user requesting the services from the cloud service provider. After completing the first stage of the security establishment process. The digital signature has been encrypted by applying the homomorphic encryption process which is used to improve the further cloud security level.

3.2 Stage 2

The second level security is established by using the homomorphic based encryption level. At the time of encryption process, user entered digital signature need to be encrypted because the signature also accessed by intermediate attacks. Normally the encryption process is performed by utilizing the private key that has been securely managed by user which is sometimes difficult to manage. So, the second level encryption process does not require the private key but it efficiently managing the data confidentiality in cloud. The homomorphic algorithm manages the digital signature authentication by using the raw credential information. The Homomorphic encryption [18] method used to perform the encryption without knowing the private key because the client only holds the secret key. The encryption is send be Fully Homomorphic Encryption if it has satisfied the following condition,

$$E(M1 \ominus M2) \Downarrow E(M1) \ominus E(M2)$$

Where M1 and M2 is the plain text which is related to the user provided digital signature information. Then the fully homomorphic encryption process is used to provide the security of the stored data in the cloud server. Then the encryption algorithm using the homomorphic encryption algorithm is defined as follows, Initially the encryption parameter has been decided and identified like r,p and q in which p is the prime number. P is the secret key. After initializing the parameters the cipher text has been computed for every plain text which is defined as follows,

$$ciphertext(c) = pq + 2r + m$$

Then the decryption is done as follows, Decrypt m= (c mod p)mod2. Finally the homomorphic encrypted cipher text has been computed as follows,

$$C_1=q_1p+2r_1+m_1 \text{ and } C_2=q_2p+2r_2+m_2$$

According to the above process, the user generated digital signature has been encrypted and stored in the cloud server. During the service access process, user verify their digital signature using the digital signature related cipher text which is only known by user that is difficult to access by intermediate person in the cloud environment. This two stages provides the security, privacy, authentication and confidentiality to the user information with effective manner which is done by using the cipher text policy attribute based homomorphic encryption algorithm. Further the security is established with the help of the image captcha verification process which is explained in the stage 3 process.

3.3 Stage 3:

The last stage of verification process is done with the help of the image captcha process. After verifying the user information and digital signature [19], the system has been randomly generates the random alphanumeric code with size 8. This code has contains some noise background image, the user need to enter this code according to the random query which is relevant to the generated image captcha. After entering the relevant code, it has to be compared to the session code, if is matched with the stored session image captcha then the user ability to access the cloud service with effective manner. This introduced query based image captcha process reduces unauthorized access also robustness. The sample image captcha related query is shown in the following figure 2.

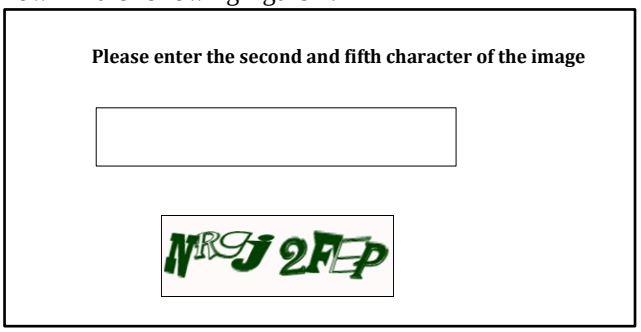

Figure 2: Process of Image Captcha

Based on the above three stage encryption and decryption process, the user sensitive information's are encrypted and stored in the cloud provider database

During the user request process, the verification is done with the relevant private key, digital signature and image captcha process. Thus the process successfully provides the security to the user sensitive information with effective manner. Then the efficiency of the system is evaluated with the help of the experimental results and discussion which is explained as follows.

4. Performance Analysis

The excellence of the proposed cipher text policy attribute based homomorphic encryption algorithm is evaluated in this section. The proposed method ensures the confidentiality, privacy, security; authorization and authentication to the user sensitive data [20] by using the three stages based authentication process. The method effectively utilizes the digital signature and image captcha which reduces the intermediate attack successfully. Then the digital signature based authentication efficiency is examined in terms of using the encryption time, execution time and cost. In this paper uses the digital signature as the important role because it does not requires the secret key during the encryption process, due to the homomorphic algorithm. This algorithm only encrypts the digital signature; the encrypted cipher text is used in the second stage of verification process. In addition, to this OTP and cipher text based encryption process ensures the additional security and privacy to the user sensitive information [21]. Further the security is evaluated in the cloud environment with the help of the security, data uploading and authentication metrics. Then the utilized efficient metrics are listed as follows.

Security
Security is important metric which is used to encrypt the user personal information with their digital signature and image captcha that helps to hide the sensitive information from the unauthorized user.

Data Sharing or Uploading
At the time of data sharing, person unique features are used to encrypt their details along with the encryption method which is difficult to hack by the third parties.

Authentication
Authentication and authorization is done with the help of the digital signature matching and image captcha entering process. In addition the method uses the secret key, access controls for maintaining the authentication with efficient manner. Then the proposed system achieves the security with minimum encryption time for user attributes which is shown in the figure 3.

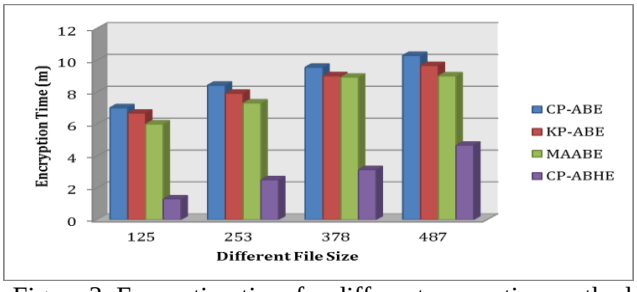

Figure 3: Encryption time for different encryption methods

From the above figure 3, it clearly shows that the proposed system consumes minimum encryption time for both small file size and large file size while requesting to upload data in the cloud environment. Then the proposed system minimize the encryption time due to efficient key management process which leads to increase the security in the cloud efficient manner. The minimum encryption time improves the overall execution time for both data sharing and security process. Then the execution time of the proposed system is shown in the figure 4.

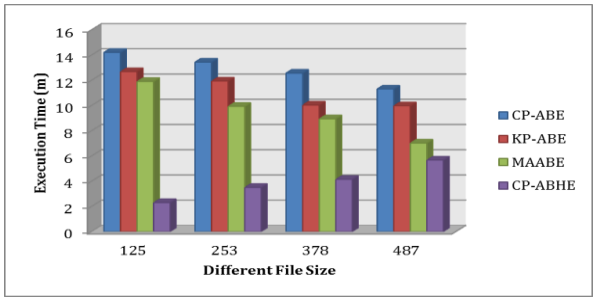

Figure 4: Execution Time for Different Encryption Methods

The above figure 4 depicted that the proposed system consumes minimum execution time for overall encrypting and permission access process. The proposed system uses the digital signature and image captcha which improves the security with efficient manner when compared to the other methods. In addition the system consumes minimum cost while providing the security to the user information. The cost consumes for the system is shown in the figure 5.

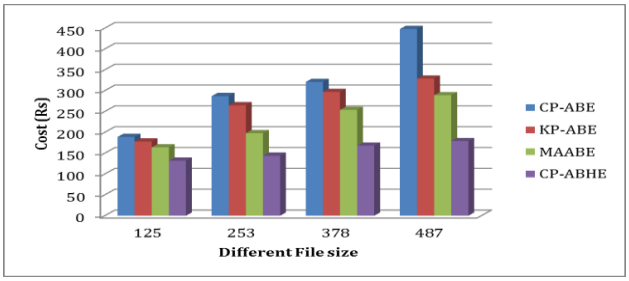

Figure 5: Cost for Different Encryption Method

The figure 5 depicted that the proposed system consumes minimum cost for different file size when compared to the existing methods. Thus the proposed system ensures the security with minimum time in the cloud environment when compared to the existing methods. So, the user details are managed successfully in the third party server.

5. CONCLUSION

Thus the paper discusses the cloud security establishment process using the OTP along with the digital signature and image captcha based encryption process which is done by using the cipher text policy attribute based homomorphic encryption algorithm. This method, enhances the security in three stages, first user sensitive information's are encrypted with the help of the cipher text policy based private key and public key. Then the user entered digital signature is encrypted and stored in the server using the homomorphic encryption method. These two process successfully ensures the security to user information. In addition, to this image captcha is used to verify the user session because the captcha works according to the query related captcha entering process. Thus the three stage encryption process effectively increases the confidentiality, privacy and security to the user information. At last the efficiency of the system is evaluated with the help of the experimental results. Thus the proposed system establishes the security with minimum time and minimum cost in the cloud environment.

REFERENCE

[1] K. Kajendran, J. Jeyaseelan, J. Joshi, "An Approach for secures Data storage using Cloud Computing" In International Journal of Computer Trends and Technology- May to June Issue 2011

[2] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE,KuiRen, Member, IEEE, and Wenjing Lou, Member, IEEE "Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE-2012

[3] K. Raen, C. Wang, Q. Wang, "Security Challenges for the Public Cloud", Published by IEEE Computer Society, Jan/Feb 2012.

[4] Kristin Lauter, Michael NaehrigandVinodVaikuntanathan, "Can Homomorphic Encryption be Practical", in ACM, 2008.

[5] ShuchengYu , "Achieving Secure, Scalable, and Finegrained Data Access Control in Cloud Computing", in Proceedings of IEEE Infocomm, ISSN: 978-1-4244-5837-0/10, 2010

[6] KawserWazedNafi, TonnyShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[7] H. Ahn, H. Chang, C. Jang and E. Choi, "User Authentication Platform using Provisioning in Cloud Computing Environment", Advanced Communication and Networking, (2011), pp. 132-138.

[8] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing", In INFOCOM, 2010 Proceedings IEEE, IEEE, (2010), pp. 1-9.

[9] Greveler U, Justus b et al. (2011). A Privacy Preserving System 2. for Cloud Computing, 11th IEEE International Conference on Computer and Information Technology, 648–653.

[10] Elisa Bertino , Federica Paci , Rodolfo Ferrini , Ning Shang ,Privacy-preserving Digital Identity Management for Cloud Computing, Copyright 2009 IEEE

[11] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol I, WCE 2012, July 4 - 6, 2012.

[12] Recordon, D., Reed, D.: OpenID 2.0: a platform for user-centric identity management. In: Proceedings of the Second ACM Workshop on Digital Identity Management, pp. 11–16. ACM, Alexandria (2006).

[13] Shobha Rajak, Ashok Verma, "Secure Data Storage in the Cloud using Digital Signature Mechanism", International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 4, June 2012.

[14] Shivam Patole, Anwar Sarkeja, "Hybrid Approach for Cloud Storage with Attribute based Encryption", International Journal of Computer Applications, Volume 154 – No.1, November 2016.

[15] Prachi Soni, MonaliSahoo, "Multi-factor Authentication Security Framework in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, volume 5,issue 1,2015.

[16] Pugazhenthi, SreeVidya, "Multiple Biometric Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, volume 3, issue 4.

[17] Vijaya Lekshmi ; M. P. Revathi, "Implementing secure data access control for multi-authority cloud storage system using Ciphertext Policy-Attribute based encryption", Information Communication and Embedded Systems (ICICES).

[18] Naoto Miura, Akio Nagasaka, "Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles", Conference on Machine VIsion Applications, May 16-18, 2005 Tsukuba Science City, Japan.

[19] Kumar, S.S. and Inbarani, H.H. (2013) 'Analysis of mixed c-means clustering approach for brain tumour gene expression data', Int. J. of Data Analysis Techniques and Strategies, Vol. 5, No. 2, pp.214–228.

[20] Cheng-Bo Yu, Hua-Feng Qin, Lian Zhang, Yan-Zhe Cui, "Finger-vein image recognition combining modified hausdorff distance with minutiae feature matching", J. Biomedical Science and Engineering, 2009, 2, 261-272.

[21] Sultan Ullah, Zheng Xuefeng, Zhou Feng, "TCloud: A Dynamic Framework and Policies for Access Control across Multiple Domains in Cloud Computing", International Journal of Computer Applications (0975 – 8887), Volume 62– No.2, January 2013.