EFFECTIVE AND SAFE BIOMETRIC-BASED CLOUD SERVICE ACCESS MECHANISM DESIGN

CHADUVULA SARATH SAINATH REDDY[1]

M.C. BHANU PRASAD[2]

C. NAGESH[3]

[1]M Tech Student, [2]Assistant Professor, Department of Software Engineering, Tadipatri Engineering College

[3]Assistant Professor, Department of CSE, Srinivasa Ramanujan Institute of Technology

chaduvula99sai@gmail.com[1], bhanuprasad01.nbl@gmail.com[2], nageshc.cse@srit.ac.in[3]

ABSTRACT: In current days cloud computing is providing great flexibility for the end- users to store and access a lot of valuable information to and from remote servers. As we all know that data is uploaded into the cloud is outsourced to a third party untrusted remote server, privacy for that data is almost a big problem for the enterprises. Hence in this current project, we try to add a new level of security for the cloud data by adding biometric authentication techniques like fingerprint images and then verify the user authentication based on the biometric images. Here we try to design a mutual authentication scheme based on bio-metric based secure access scheme for cloud computing to avoid the illegal data access by unauthorized users and in which this will be divided into two phases for providing security. In first phase the user is asked to choose bio metric authentication in the form of finger print images and in the second phase the owner can upload bio metric related data into the cloud server in a secure manner by encrypting the files using cryptography algorithms.

Keywords: Authentication, biometric-based security, cloud service access, session key.

I. INTRODUCTION

Cloud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], O Auth [2] and OpenID [3] (see [1], [4] – [12]). Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network. Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server. Once both verifications are successfully carried out, the user obtains access to the services from some remote server. One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols of Jiang et al. [13], Althobaiti et al. [14], Xue et al. [15], Turkanovic et al. [16], Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19] and Kang et al. [20] – see also Section II. Therefore, in this paper we seek to design a secure and efficient authentication protocol. Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information. In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server.

To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key.

Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometric based message authenticator is also generated for message authenticity purpose. We summarize the key contributions/benefits related to the proposed approach as below. 1) An effective way to transmit the user's biometric data through the unsecured network channels to an authentication server is presented. 2) We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere. 3) We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server. 4) We introduce a novel way to generate session keys. 5) In traditional authentication protocol, each entity requires some preloaded information; thus, incurring some overhead. We introduce a new mechanism to avoid the need for secret pre-loaded information. 6) A message authentication mechanism, as an alternative to the existing message authentication protocols (i.e., Message Authentication Code (MAC)), is introduced. In the next section, we will review existing biometric based authentication schemes, prior to presenting the proposed biometric-based authentication approach in Section III. We then evaluate the performance and security of the proposed protocol in Sections IV and V, respectively. Specifically, we demonstrate that the protocol is secure in the presence of a DolevYao (DY) adversary [21].

II. RELATED SYSTEM

A few authentication components have been proposed in the writing, for example, those based on Kerberos [6], OAuth [7], and OpenID [8]. For the most part, these protocols look to set up a protected assigned access instrument among two conveying elements associated in an appropriated framework. These protocols are based on the fundamental presumption that the distant server answerable for authentication is a confided in substance in the organization. In particular, a client first registers with a far off server. This is expected to guarantee the approval of the proprietor. At the point when a client wishes to access a server, the distant server confirms the client and the client additionally validates the server. When the two confirmations are effectively done, the client gets access to the services from some distant server. One key restriction in existing authentication components is that the client's accreditations are put away in the authentication server, which can be taken and (mis)used to acquire unapproved access to different services. Additionally, to guarantee secure and quick correspondence, existing systems for the most part utilize symmetric key cryptography, which requires a few cryptographic keys to be shared during the authentication cycle. This methodology brings about overhead to the authentication protocols. Consequently, in this paper, we look to plan a protected and proficient authentication protocol. In particular, we will initially give an option in contrast to the traditional secret word based authentication system. At that point, we show how one can construct a safe correspondence between conveying parties associated with the authentication protocol, without having any mystery pre-stacked (i.e., shared) data.

III. PROPOSED SYSTEM

In the proposed approach, we consider a fingerprint picture of a client as a mystery qualification. From the fingerprint picture, we create a private key that is utilized to enlist the client's certification covertly in the database of an authentication server. In the authentication stage, we catch another biometric fingerprint picture of the client, and hence produce the private key and scramble the biometric data as a question. This questioned biometric data is then communicated to the authentication server for coordinating with the put away data. When the client is validated effectively, he/she is prepared to access his/her service from the ideal server. To get secure access to the service server, common authentication between the client and authentication server, and furthermore between the client and service server have been proposed utilizing a transient session key. Utilizing two fingerprint data, we present a quick and powerful way to deal with create the session key [1]. Likewise, a biometric-based message authenticator is produced for message realness purposes.

In this segment, we initially talk about the system model and threat model utilized in the proposed biometric-based authentication protocol (BioCAP), prior to introducing the different stages in BioCAP. A. System Model An outline of BioCAP is appeared in Fig. 3, which involves three elements. These elements are the client(s) (C), authentication server(s) (AS), and some asset server (RS). AS contains a database of clients' enlisted data, while AS creates RS's private key during the sending stage and it is divided among AS and RS. Likewise, both AS and RS incorporate an enormous vault of a comparative arrangement of engineered fingerprint pictures. Some manufactured fingerprint databases, for example, some openly accessible databases, are utilized in the proposed approach. At the point when C wishes to access a service from RS, C initially sends an authentication solicitation to AS. AS checks C's solicitation and sends an answer message to C upon fruitful confirmation. When C acquires the authentication answer message, C sends a service solicitation to RS for getting access. RS at that point confirms the service demand. On the off chance that the service demand is confirmed effectively, RS sends an answer to C. C and RS commonly validate one another. A session key among C and AS, and C and RS are utilized for resulting secure message interchanges. Further, the message legitimacy is constrained by a message authenticator. BioCAP has two key cycles, to be specific: client enrollment and client authentication. The client enlistment requires a private key generation, though client authentication requires the generation of the session key and the message authenticator. BioCAP gives an arrangement to turn over the private key of a client. Additionally, BioCAP is secure, computationally more affordable, and defeats the inborn shortcomings of biometric confirmation. Also, BioCAP doesn't require pre shared keys, and gives a smooth common authentication system, and requests less number of keys to be overseen from application and client perspective.

IV. EXPERIMENTAL RESULTS

In this section we try to design our current model using Java as programming language and taking MY-SQL as storage database. Here the front end of the application is designed using JSP and HTML and back end we used My-SQL server. Now we can check the performance of our proposed application as follows:

Performance Comparison with Other User Authentication Schemes We compare the performance of our approach with the existing biometric-based user authentication schemes of Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19], and Kang et al. [20]. In this section, we use the same evaluation metrics used in the studies of [61]–[66]. We compare the communication costs comparison among the proposed scheme and other schemes [17], [18], [19], [20] in Table VI. We apply the following assumptions to compute the number of bits needed for transmission of the messages during the login and authentication phases: biometric index Bx is 164 bits, secret K0 r is 128 bits, secret K0 c is 128 bits and F 0 qry is 128 bits. Therefore, during authentication, in first message we send 288 bits long message and in second message of 256 bits long message. The communication costs needed for the schemes of Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19], and Kang et al. [20] are 2528 bits, 3040 bits, 704 bits and 960 bits, respectively.

V. CONCLUSION

In this paper, we for the first time designed a model to add a new level of security for the cloud data by adding biometric authentication techniques like fingerprint images and then verify the user authentication based on the biometric images. Here we try to design a mutual authentication scheme based on a smartcard for cloud computing to avoid the illegal data access by unauthorized users and in which this will be divided into two phases for providing security. By conducting various experiments on our proposed method we finally came to an conclusion that our proposed method of smartcard authentication system can able to give high level of security for the users who try to access the sensitive information like iris related data in a secure manner and we can also able to restrict the un-authorized users not to enter the others account and try to view the data illegally.

REFERENCES

[1] C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authentication service (v5),” RFC 4120, 2005.

[2] “OAuth Protocol.” [Online]. Available: http://www.oauth.net/

[3] “OpenID Protocol.” [Online]. Available: http://openid.net/

[4] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[5] A. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.

[6] B. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.

[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon : endto-end authorisation support for resource-deprived environments,” IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.

[8] S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” Washington D.C., USA, October 2003, pp. 62–72.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS: security protocols for sensor networks,” ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.

[10] P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.

[11] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kesrberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[12] M. Walla, “Kerberos explained,” Windows 2000 Advantage Magazine, 2000.

[13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015.

[14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, “An efficient biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013, Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971.

[15] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.

[16] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," Ad Hoc Networks, vol. 20, pp. 96 – 112, 2014.

[17] M. Park, H. Kim, and S. Lee, "Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards," in 17th International Conference on Computational Science and Engineering, Chengdu, China, 2014, pp. 1541–1544.

[18] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255 – 270, 2017.

[19] S. D. Kaul and A. K. Awasthi, "Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement," Wireless Personal Communications, vol. 89, no. 2, pp. 621–637, 2016. 69

[20] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient and Secure Biometric-Based User Authenticated Key Agreement Scheme with Anonymity," Security and Communication Networks, vol. 2018, pp. 1–14, 2018, Article ID 9046064, https://doi.org/10.1155/2018/9046064.

[21] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.