



A Novel Implementation Of Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services

SHAIK RESHMA¹, A.SURENDRA BABU²

#1Student, Dept of CSE, VelagaNageswaraRao College Of Engineering,
Ponnur(Post),Ponnur(Md)Guntur(D.T)A. Andhra Pradesh.

#2Assoc Professor, Dept of CSE, VelagaNageswaraRao College Of Engineering,
Ponnur(Post),Ponnur(Md)Guntur(D.T)A. Andhra Pradesh

Abstract The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal (non-mathematical) security analysis and also formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool reveal that the proposed approach can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach

1.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 researchwise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [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.

2. LITERATURE SURVEY

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

This document provides an overview and specification of Version 5 of the Kerberos protocol, and it obsoletes [RFC 1510](#) to clarify aspects of the protocol and its intended use that require more detailed or clearer explanation than was provided in [RFC 1510](#). This document is intended to provide a detailed description of the protocol, suitable for implementation, together with descriptions of the appropriate use of protocol messages and fields within those messages.

[2] "OAuth Protocol." [Online]. Available: <http://www.oauth.net/>

The [OAuth 2.0](#) specification defines a *delegation* protocol that is useful for conveying *authorization decisions* across a network of web-enabled applications and APIs. OAuth is used in a wide variety of applications, including providing mechanisms for user authentication. This has led many developers and API providers to incorrectly conclude that OAuth is itself an *authentication* protocol and to mistakenly use it as such. Let's say that again, to be clear:

OAuth 2.0 is not an authentication protocol.

Much of the confusion comes from the fact that OAuth is used *inside* of authentication protocols, and developers will see the OAuth components and interact with the OAuth flow

and assume that by simply using OAuth, they can accomplish user authentication. This turns out to be not only untrue, but also dangerous for service providers, developers, and end users.

This article is intended to help potential *identity providers* with the question of how to build an authentication and identity API using OAuth 2.0 as the base. Essentially, if you're saying "I have OAuth 2.0, and I need authentication and identity", then read on.

[3] "OpenID Protocol." [Online]. Available: <http://openid.net/>

OpenID Authentication provides a way to prove that an end user controls an Identifier. It does this without the Relying Party needing access to end user credentials such as a password or to other sensitive information such as an email address.

OpenID is decentralized. No central authority must approve or register Relying Parties or OpenID Providers. An end user can freely choose which OpenID Provider to use, and can preserve their Identifier if they switch OpenID Providers.

While nothing in the protocol requires JavaScript or modern browsers, the authentication scheme plays nicely with "AJAX"-style setups. This means an end user can prove their Identity to a Relying Party without having to leave their current Web page.

OpenID Authentication uses only standard HTTP(S) requests and responses, so it does not require any special capabilities of the User-Agent or other client software. OpenID is not tied to the use of cookies or any other specific mechanism of Relying Party or OpenID Provider session management. Extensions to User-Agents can simplify the end user

interaction, though are not required to utilize the protocol.

The exchange of profile information, or the exchange of other information not covered in this specification, can be addressed through additional service types built on top of this protocol to create a framework. OpenID Authentication is designed to provide a base service to enable portable, user-centric digital identity in a free and decentralized manner.

3.PROPOSED SYSTEM

In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information.

3.1 IMPLEMENTATION

Data Owner

In this module, the data owner uploads their Biometric images with their contents data to the Cloud server. For the security purpose the data owner assigns the digital sign and then store in the Cloud and also performs the following operations such as Upload Biometric image with its digital sign based on title, desc, List all uploaded Biometric images, Verify Biometric image details, and Delete Biometric image details

Cloud Server

The Cloud service provider manages a Cloud to provide data storage service. And performs the following operations such as Store all Biometric image files with their signature, View all Biometric image Files with its details, View all Biometric image comments, View all Data owners and Users, and View all attackers

Users

The Cloud User who has a large amount of data to be stored in Cloud Servers and have the permissions to access and manipulate stored Biometric image and its data. The consumer will search the data and accessing the Biometric image data if he is authorized and performs the following operations such as Search Biometric image , Access Biometric image and its details, Download Biometric image & make comments

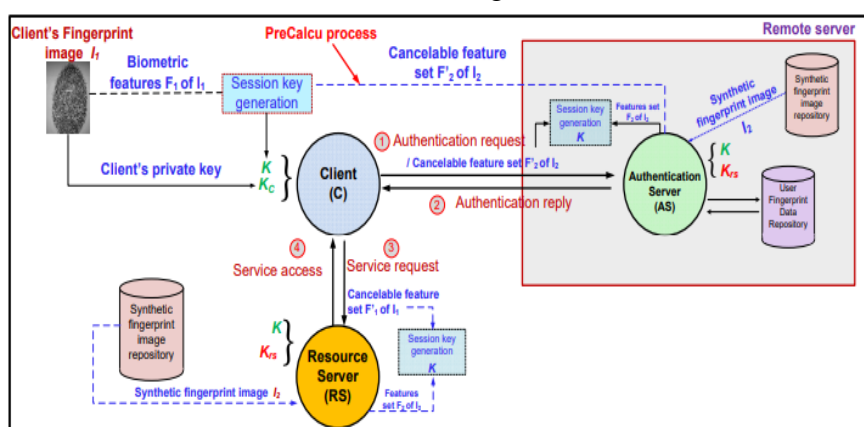


Fig: 1. System Model

4.RESULTS AND DISCUSSIONS

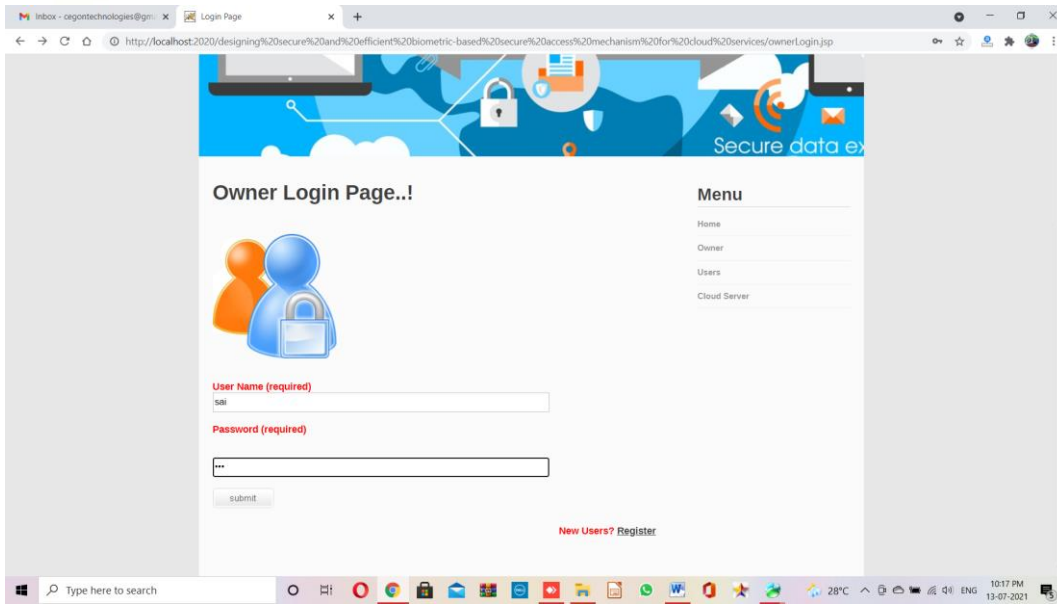
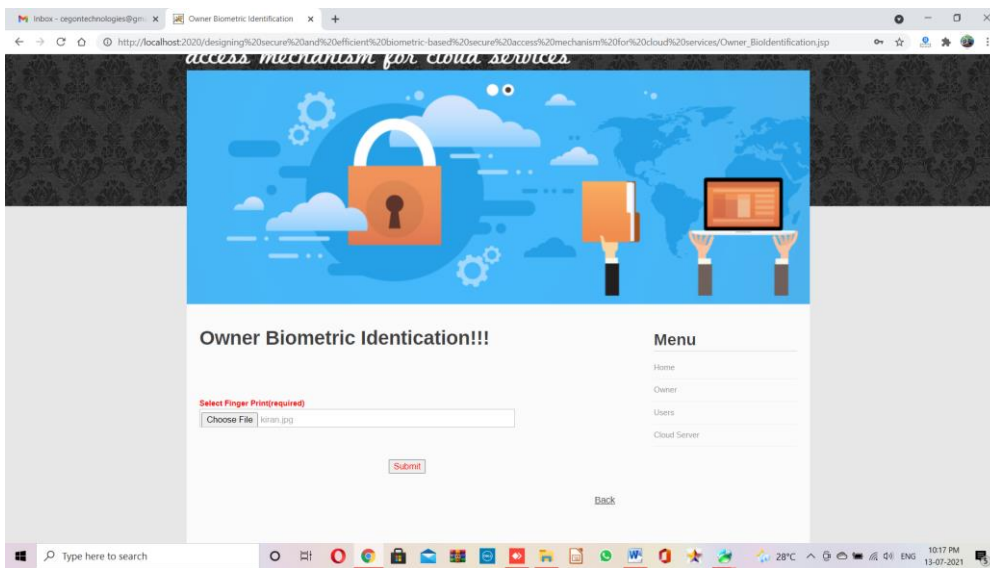


Fig 4.1 Owner Login Form



Fog 4.2 in this page owner needs provide biometric image for login if the image is correct then owner can view his actions

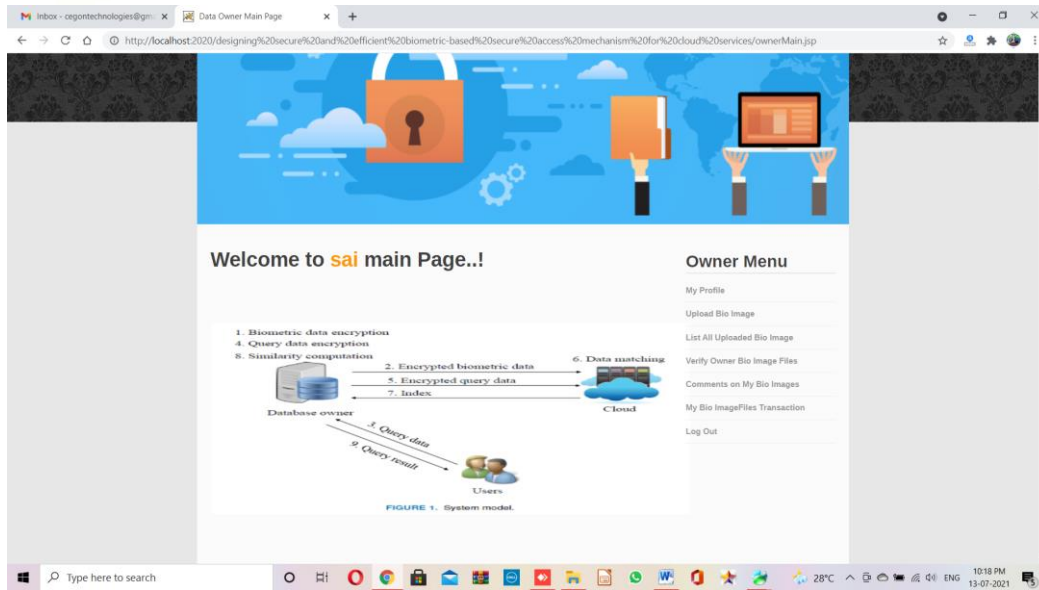


Fig 4.3 owner main page

4.CONCLUSION

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and computational resources from a remote location. Our proposed approach allows one to generate a private key from a fingerprint biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy. Our proposed session key generation approach using two biometric data does not require any prior information to be shared. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks. Future research includes exploring other biometric traits and also multi-modal biometrics for other sensitive applications (e.g., in national security matters)

FUTURE SCOPE

Future research includes exploring other biometric traits and also multi-modal

biometrics for other sensitive applications (e.g., in national security matters).

REFERENCES

- [1] A. Jain, L. Hong and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 43, no. 2, pp. 90-98, 2000.
- [2] R. Allen, P. Sankar and S. Prabhakar, "Fingerprint identification technology," Biometric Systems, pp. 22-61, 2005.
- [3] J. de Mira, H. Neto, E. Neves, et al., "Biometric-oriented Iris Identification Based on Mathematical Morphology," Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195, 2015.
- [4] S. Romdhani, V. Blanz and T. Vetter, "Face identification by fitting a 3d morphable model using linear shape and texture error functions," in European Conference on Computer Vision, pp. 3-19, 2002.
- [5] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Journal of Computer



Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.

[6] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24-34, 2007.

[7] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications Magazine*, vol. 15, no. 4, pp. 60-66, 2008.

[8] X. Hei, and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergency," in *Proc. of IEEE INFOCOM 2011*, pp. 346-350, 2011.

[9] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. of IEEE GLOBECOM 2010*, pp. 1-5, 2010.

[10] M. Barni, T. Bianchi, D. Catalano, et al., "Privacy-preserving fingerprint authentication," in *Proceedings of the 12th ACM workshop on Multimedia and security*, pp. 231-240, 2010.

[11] M. Osadchy, B. Pinkas, A. Jarrous, et al., "SCiFI-a system for secure face identification," in *Security and Privacy (SP), 2010 IEEE Symposium on*, pp. 239-254, 2010.

Author's Profile



Shaik Reshma pursuing M. Tech in Computer Science and Engineering from Velaga Nageswara Rao College Of Engineering, Ponnur. Affiliated to JNTUK, KAKINADA.



A. Surendra babu Qual : MTECH _CSE, designation : Assoc.Prof, exp : 7 year's.