JES
Journal of Engineering Sciences
Vol 13, Issue 06, June /2022
ISSN NO:0377-9254

A Novel Implementation Of Secure and Efficient Biometric-Based Secure Access Mechanism for different cloud services

Anusha Bondili[1], Nagamallikarjuna N[2]

#1Assistant Professor,Dept. Of CSE, Chebrolu Engineering College, Guntur

#2Student, Dept. Of CSE, Chebrolu Engineering College, Guntur

Abstract_ Increasing demand for remote data storage and computation services necessitates the requirement for safe access to such data and services. Here, we propose a new biometric authentication system for securing access to a distant server (in the cloud). We use biometric data as a secret credential in the suggested method. Using the user's biometric data, we can then create a unique identity from which the private key can be generated. Using two biometric templates, we devise a fast method for generating a secure message transmission session key between two parties. There is no need to store the user's private key, and the session key is produced without sharing any prior information. Security analysis using the widely accepted Automated Validation of Internet Security Protocols and Applications tool (AVISPA) and the Real-Or-Random model based on formal, informal (non-mathematical) and formal security analysis show that the proposed approach can resist several known attacks against (passive/active) adversary. Extensive experiments and a comparative investigation show that the proposed method is both efficient and effective.

1.INTRODUCTION:

We live in a world where cloud services are the standard. To be sure, designing robust authentication, authorization and accounting for access to cloud services isn't an easy task either operationally or research-wise. OpenID and Kerberos [1], OAuth [2] and Kerberos [3] are just a few of the many authentication methods that have been discussed in the literature over the years. There are several types of protocols aimed at making it possible for two communicating entities in a distributed system to securely transfer access rights. Since the distant server that performs authentication is assumed to be a reliable part of the network, these protocols are predicated on that

premise. First, a user connects to a distant server. This is necessary to guarantee that the owner has the authority to do so. The distant server authenticates the user and the user authenticates the server while accessing a server. Once both checks have been completed successfully, a remote server grants the user access to the requested services. Users' credentials can be stolen and (mis)used to obtain unauthorised access to numerous services through existing authentication systems. Existing techniques typically use symmetric key cryptography, which necessitates the exchange of multiple cryptographic keys throughout the authentication process in order to assure both security and speed. As a result of this method, the authentication procedures incur additional overhead. As evidenced by the weaknesses revealed in the published protocols of Jiang et al. [13], Althobaiti et al. [14], Xue and colleagues [15], Turkanovic and colleagues [16], Park and collaborators [17], Dhillon and Kalra and colleagues [18], Kaul and Awasthi and colleagues [19] and Kang and colleagues [20] – see also Section II – designing secure and efficient authentication protocols is difficult. This paper's goal is to provide an authentication system that is both safe and fast. As a starting point, we'll offer an alternative to password-based authentication. Finally, we illustrate how to construct a secure connection between communicating parties engaged in the authentication protocol, without having any secret pre-loaded (i.e, shared) information available..

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

Architecture Diagram

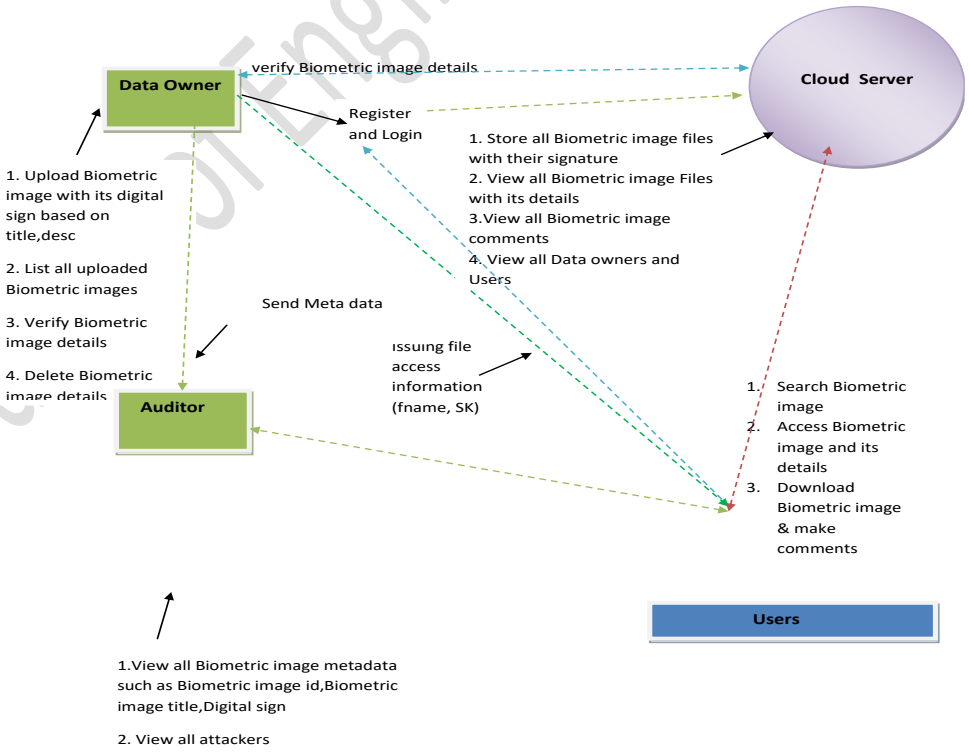


Fig: 1. System Model

Journal of Engineering Sciences
Vol 13, Issue 06, June /2022
ISSN NO:0377-9254

4.RESULTS AND DISCUSSIONS

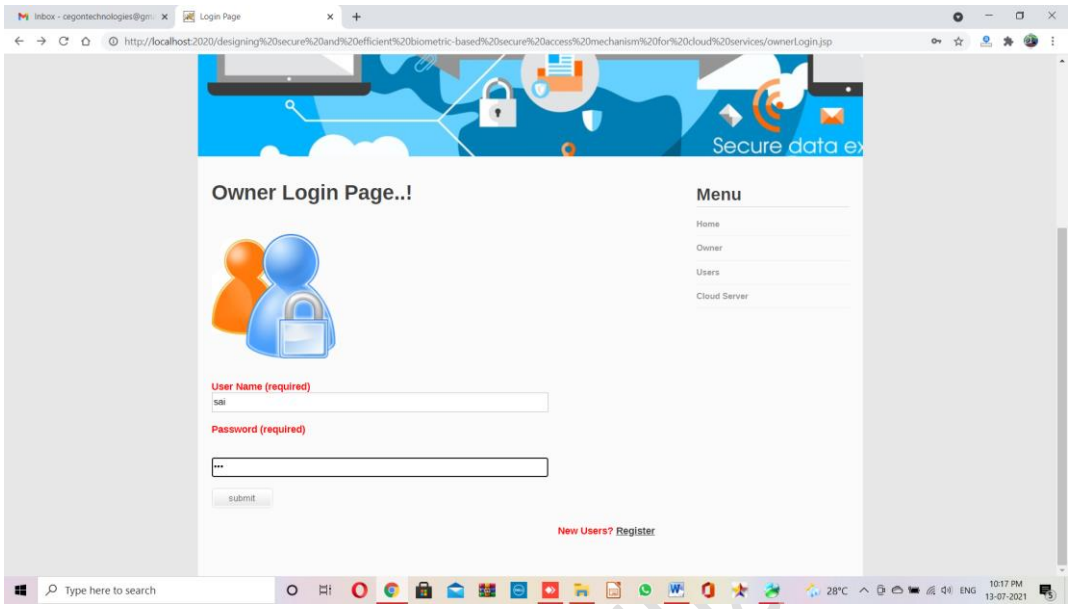
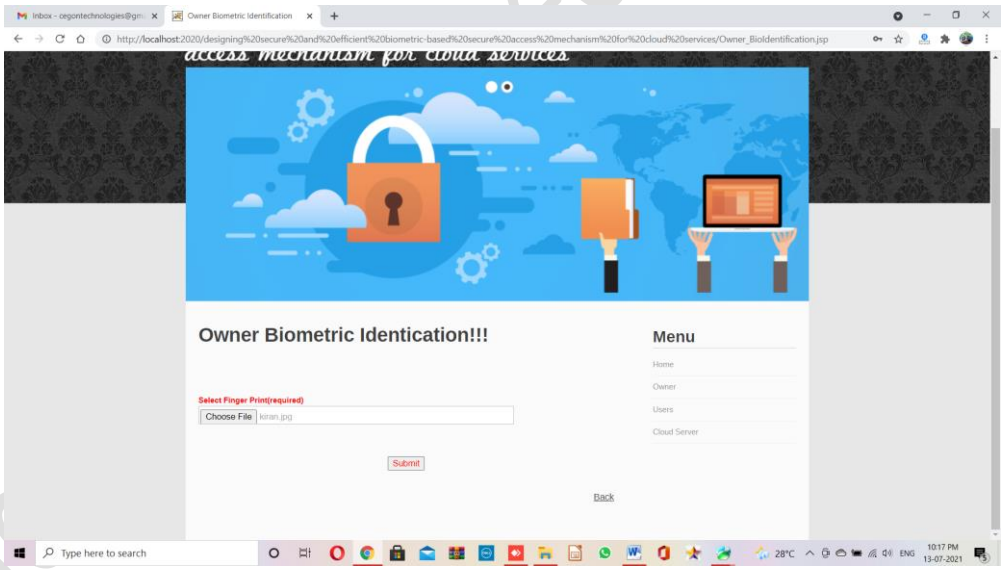


Fig 4.1 Owner Login Form



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

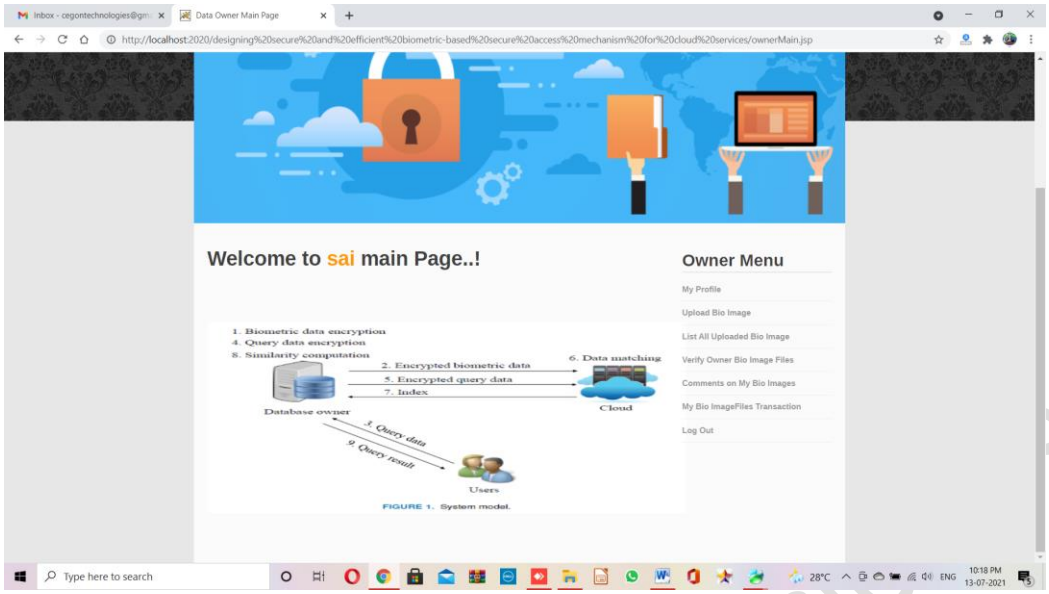


Fig 4.3 owner main page

4.CONCLUSION

As indicated by the rising use of biometrics over more traditional security measures like passwords and tokens (e.g., on Android and iOS devices). To authenticate a user who wants to use services and computing resources from a remote place, we developed a biometric-based technique. Because a user's fingerprint can be used to produce the identical private key with an accuracy of 95.12 percent, we believe our approach is viable. Using two biometric data to generate a session key does not necessitate the sharing of any prior information. Compared to previous authentication systems, our method is more resistant to a number of well-known threats. Other biometric features and multi-modal biometrics for sensitive applications will be studied in the future (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,andH.H.Chen,"Aneffectivekeymanagement 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,andX.Du,"Biometric-basedtwo-levelsecureaccesscontrolforimplantable 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 implantablemedicaldevices,"inProc. ofIEEEGLOBECOM2010,pp.1-5, 2010.

[10] M. Barni, T. Bianchi, D. Catalano, et al., "Privacy-preserving fingercode 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,"inSecurityandPrivacy(SP),2010IEEESymposiumon,pp. 239-254, 2010.