AN ATTACK ON PRIVACY Via STATISTICAL INFERENCE IN A BIOMETRIC IDENTIFICATION SCHEME

Mrs.Vijaya Ramineni[1], Ms. Lavanya Damerla [2]

#1 Associate professor in the department of IT at DVR & DR. HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of Computer Applications (DCA) at DVR & DR. HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District

ABSTRACT_ Biometric identification allows people to be identified by their unique physical characteristics. Among such schemes, fingerprinting is well-known for biometric identification. Many studies related to fingerprint-based biometric identification have been proposed; however, they are based purely on heavy cryptographic primitives such as additively homomorphic encryption and oblivious transfer. Therefore, it is difficult to apply them to large databases because of the expense.

To resolve this problem 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 project, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, i consider biometric data of a user as a secret credential.I then derive a unique identity from the user's biometric data, which is further used to generate the user's private key

1.INTRODUCTION:

In today's data-driven landscape, the proliferation of remote data storage and computation services has soared, driven by the growing reliance on digital resources and the convenience they offer[1][2]. However, this expansion comes hand in hand with an escalating need for robust security measures to safeguard sensitive information stored in remote cloud servers. Traditional methods of authentication, such as passwords and PINs, are increasingly susceptible to sophisticated cyber threats, necessitating innovative solutions that can withstand evolving security challenges[3].

In response to this pressing demand, this paper introduces a cutting-edge biometric-based authentication protocol tailored specifically for securing access to remote cloud servers[4]. Biometric authentication, harnessing unique physical characteristics such as fingerprints or facial features, offers a promising avenue for enhancing security while streamlining user

access. Our proposed protocol leverages the inherent uniqueness of biometric data to establish a secure authentication framework, where the user's biometric information serves as a secret credential.Central to our approach is the generation of a unique identity from the user's biometric data, which in turn forms the basis for deriving a private key for secure access to cloud services. Unlike conventional methods that require storing private keys on servers, our protocol eliminates this vulnerability by generating session keys dynamically during communication, based on biometric templates shared between parties. This not only enhances security but also mitigates the risk of key compromise[6][7].To validate the effectiveness and robustness of our proposed protocol, we conduct a comprehensive security analysis, employing both formal methodologies such as the Real-Or-Random (ROR) model and state-of-the-art verification tools like the Automated Validation of Internet Security Protocols and Applications (AVISPA). Through rigorous testing, we demonstrate the protocol's resilience against a spectrum of known attacks orchestrated by passive and active adversaries[8][9].

Furthermore, we present extensive experimental evaluations and comparative studies to assess the efficiency and utility of our biometric-based authentication protocol in real-world scenarios[11]. By elucidating its performance advantages and practical implications, we aim to underscore the pivotal role of biometrics in fortifying cloud security and meeting the escalating demands of modern data access paradigms[10].

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

a brand-new biometric authentication mechanism to offer safe access to a distant server in the cloud. The suggested method treats a user's biometric information as a secret credential. The user's biometric information is then utilised to create a unique identity, which is subsequently used to create the user's private key. Furthermore, we provide a productive method for creating a secret key that allows two interacting parties to send secure messages by utilising two biometric templates. Users can safely access the data based on that key.

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

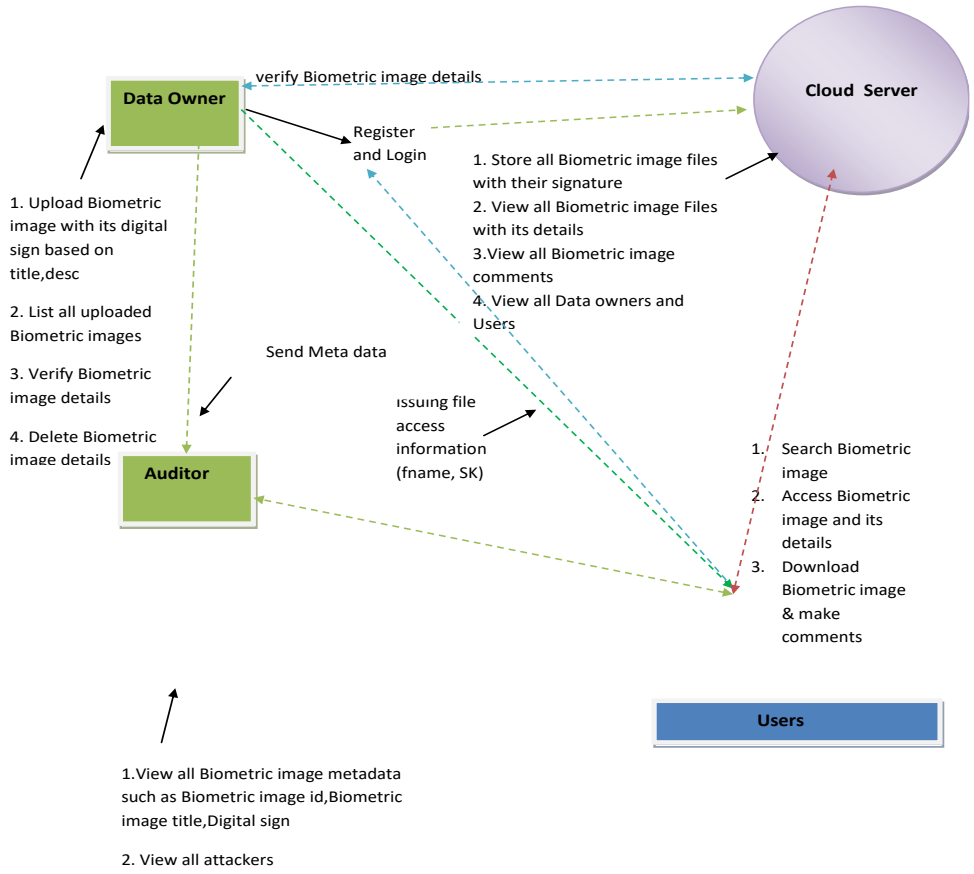
The Cloud service provider manages a Cloud to provide data storage service. And performs the following operations such as Store all Biometric image files with their signature, View all Biometric image Files with its details, View all Biometric image comments, View all Data owners and Users, and View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

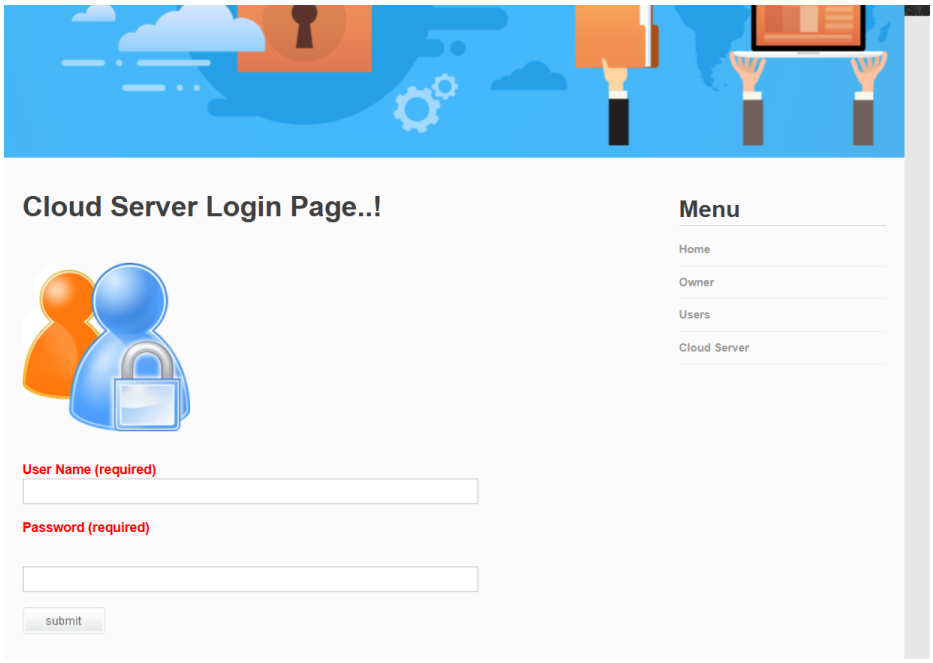


.

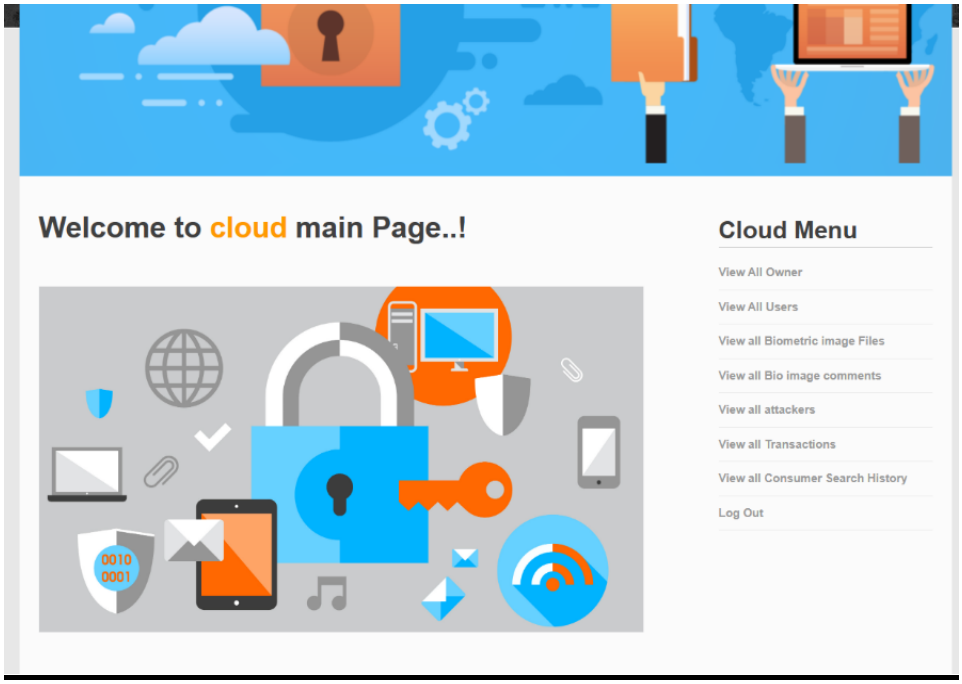
Fig: 1. System Model

4.RESULTS AND DISCUSSION

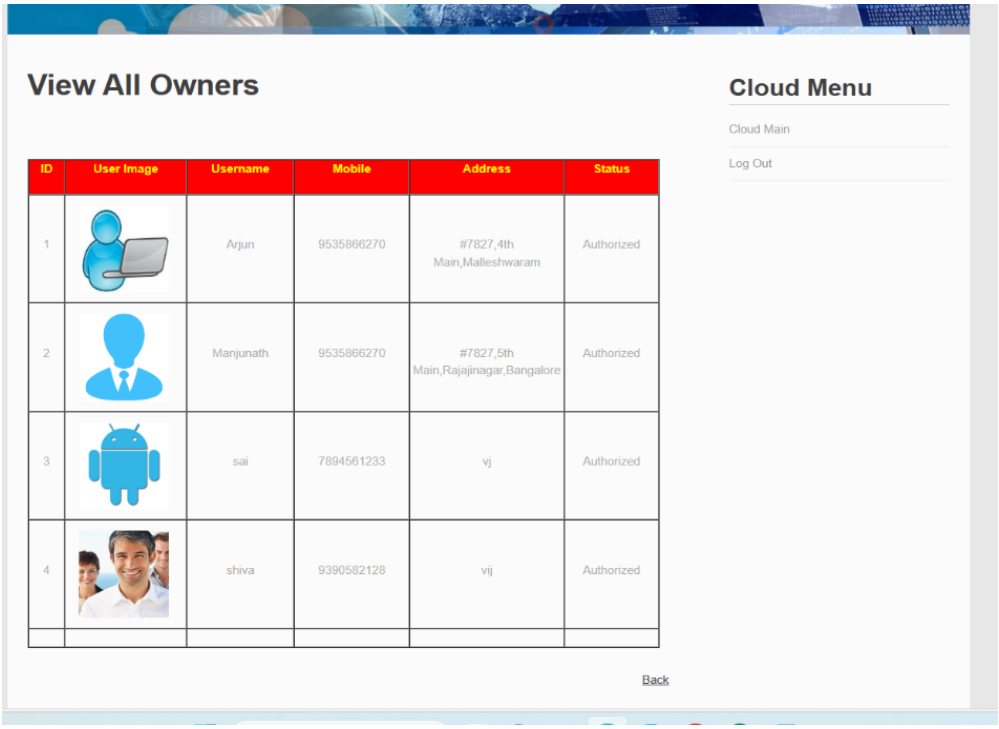
Home Page



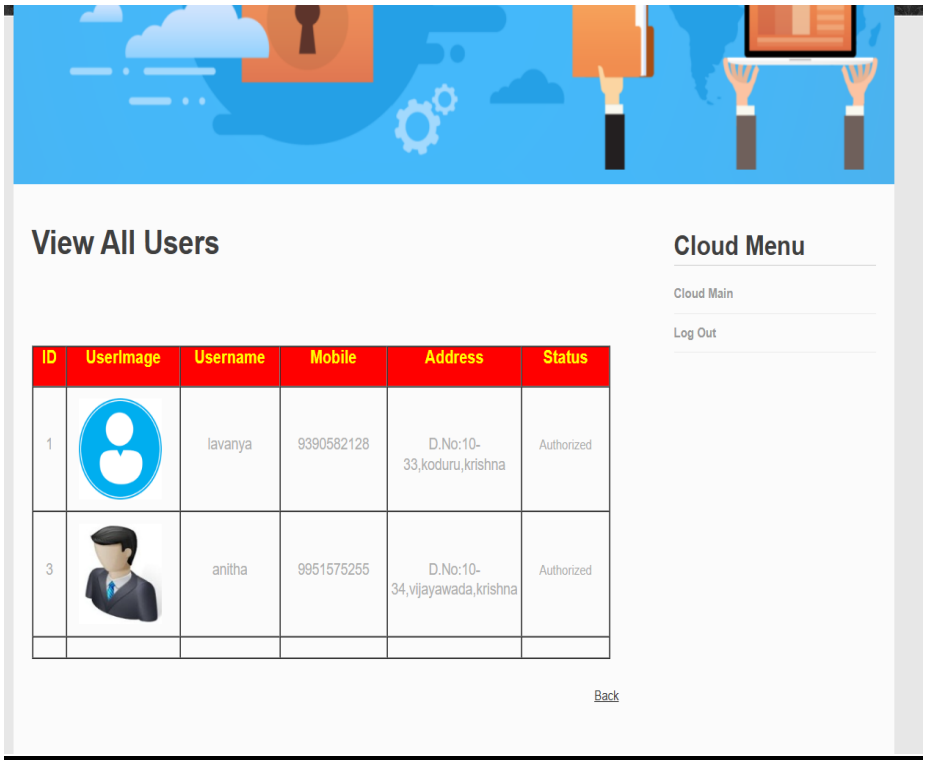
Cloud Login Page



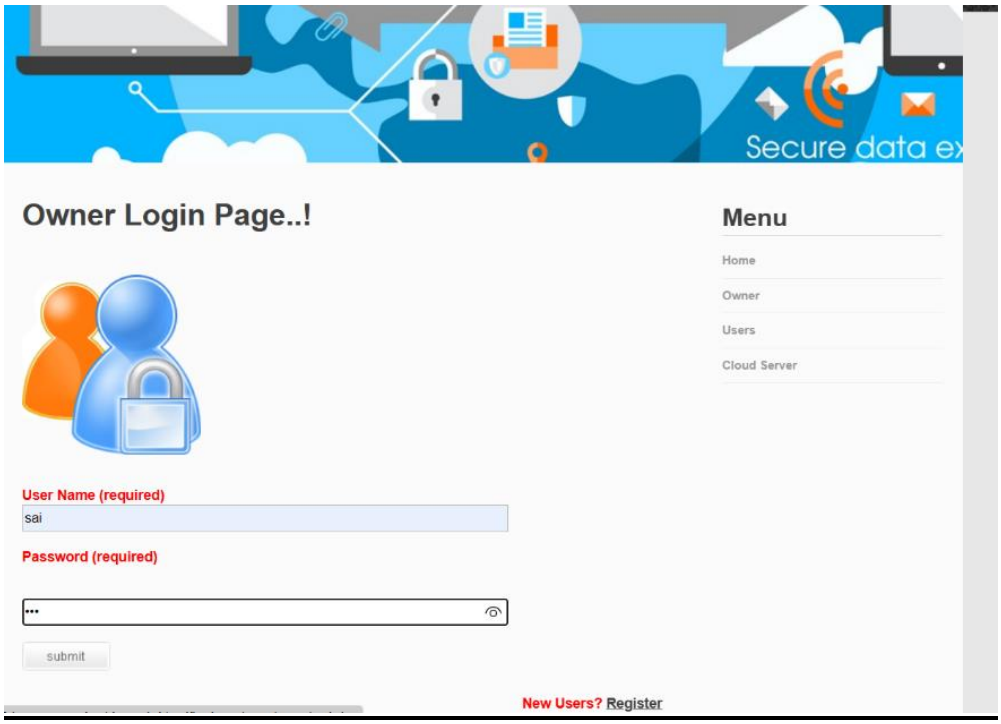
Cloud Main Page



List Of All Owners

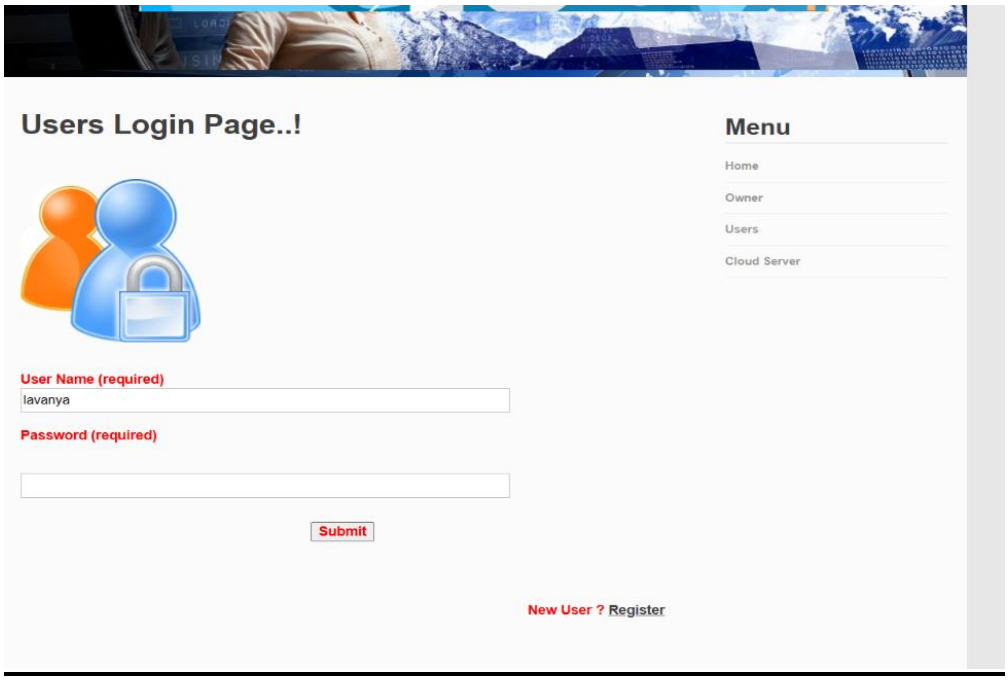


List Of All Users

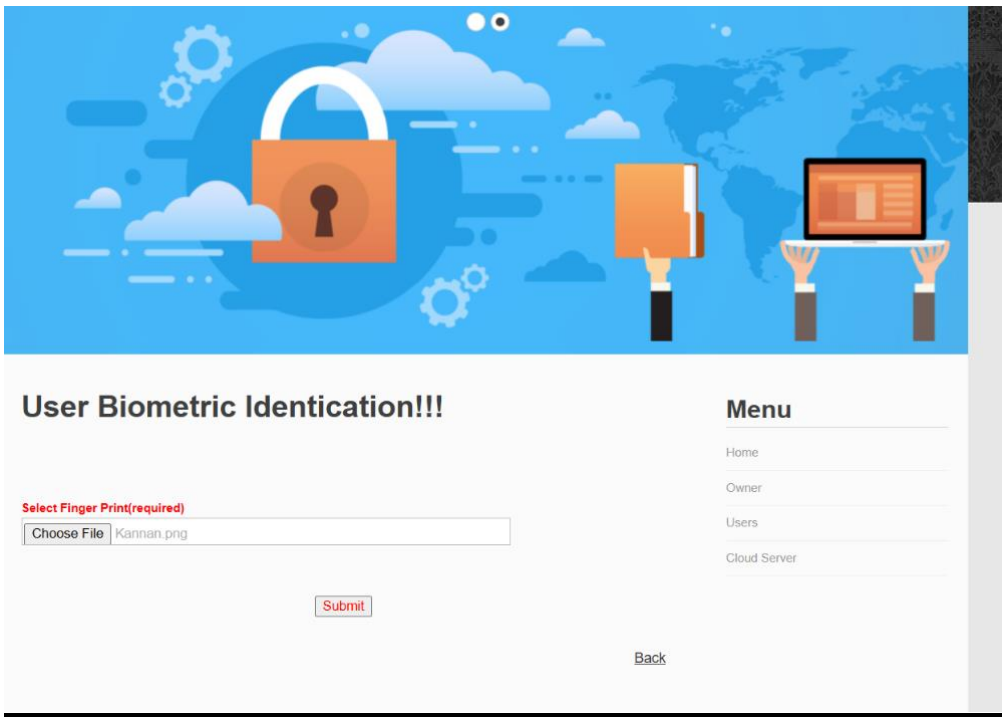


Owner Login Page

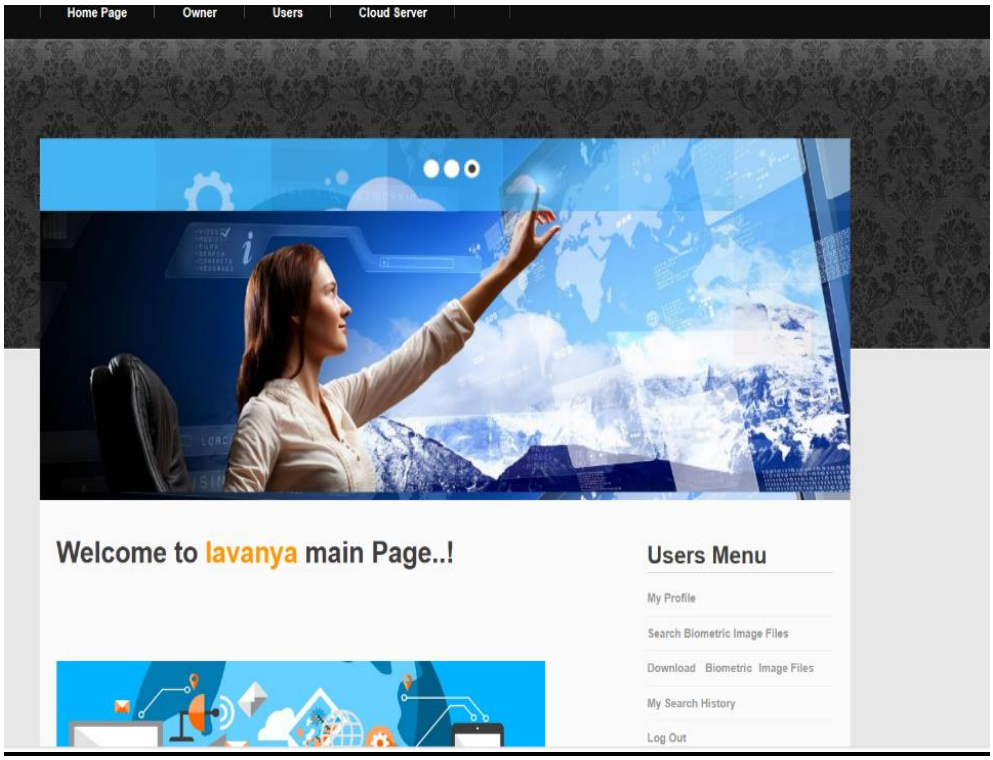
New Owner Register Page



User Login Page



Biometric Identification



User Home Page

5.CONCLUSION

Biometric security systems are becoming more and more popular, as demonstrated by their distinct advantages over traditional password- and token-based systems (e.g., on Android and iOS devices).

In order to authenticate a user attempting to access services and computing resources from a remote place, I devised a biometric-based approach in this project. Since a user's fingerprint may be used to produce the same key with 95.12% accuracy, my suggested method makes it possible to construct a private key from fingerprint biometric reveals.

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-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 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.

AUTHOR PROFILE

Mrs.Vijaya Ramineni completed her Master of computer Applications(MCA), M.Tech in (CSE) from Acharya Nagarjuna University. She has published more than 10 papers in indexing journals, Currently working as an Associate professor in the Department of IT at DVR & DR. HS MIC College of Technology(Autonomous), Kanchikacherla, NTR (DT). Her areas of interest include Data Mining,Cloud Computing and Machine Learning.

Ms. Lavanya Damerla, as MCA student in the department of DCA at DVR & DR. HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR (DT). She has completed B.Sc (MPCs) in Maruti Degree College From KRISHNA UNIVERSITY. Her areas of interests are web Development,Java, Cloud Computing.