Biometric-Based Secure Access Mechanism for Cloud Services

[1] Vangapally Geetha, [2]Dr.N.Chandra Mouli

[12] Vaageswari College of Engineering, Telangana, India

[1]geethavangapally@gmail.com [2] cmnarsingoju@gmail.com

ABSTRACT

Recent years have seen a rapid development of biometric identification due to its convenience and trustworthiness. Numerous sequestration-preserving biometric identifying methods have been proposed, utilizing either homomorphic encryption or matrix-metamorphosis, because to the perceptibility of biometric data. However, homomorphic encryption-based techniques typically have low computational efficacy, whereas matrix metamorphosis-based schemes are legitimately secure. In this study, we show that a known-plaintext attack can compromise the recently suggested matrix- metamorphosis-grounded sequestration- preserving biometric identification technique by Zhu et al (KPA). We provide a new sequestration-preserving biometric identification approach to address this security flaw, which makes use of the orthogonal matrix's feature as well as novel randomness. Security analyses and comparisons show that our system can thwart the more significant chosen-plaintext attack (CPA), which is a practical attack, as well as the KPA attack. Additionally, our system is more computationally efficient than previous comparable systems, which means it may accommodate a larger database for actual biometric identification and improve the segregation security of sensitive biometric data.

I. INTRODUCTION

Cloud Computing:

Cloud computing Internet-based subscriptions to computer resources (hardware and software) (typically the Internet). Complex architecture Is represented in system diagrams by a cloud-shaped symbol. In cloud computing, data, software, and processing are all transmitted to other services. Third-party-managed hardware and software resources over the Internet are called "cloud computing." Many of thesefirmsprovideaccesstohigh-endservernetworksandcutting-edgesoftwarepackagesforitsusers

Fig 1.1: Cloud computing

• There are consumer-oriented uses for supercomputing power that were previously reserved for the military and academic institutions. Examples of these include financial portfolios, customized information, data storage, and massively immersive computer games. These applications can perform trillions of calculations per second.

• To divide data processing tasks, the cloud computing uses large groups of computers, often running low-cost consumer PC technology with specialized networking. In today's world, the majority of computers are part of a vast network of interconnected devices. Virtualization techniques are routinely used to unlock the full potential of cloud computing.

• It includes: Features and service models:

•

• Consider these elements of cloud computing, according to NIST's definition:

•

• Rather than dealing with the service providers directly, customers can self-

provision computer resources such as server time and network storage as needed.
•
• Using standard protocols, any client system, no matter how thin or thick, can access network capabilities (e.g., mobile phones, laptops, and PDAs).
•
• Multi-tenant models allow the provider's resources to be pooled to serve many clients, with unique physical and virtual resources dynamically assigned and reassigned according to the demands of the consumers.it is common for customers to be unable or unwilling to know exactly where their purchased goods are located, but may have the option of specifying location at a more abstract level of abstraction (e.g., country, state, or data center). Resources include virtual machines, storage, processing, and network band width.
•
• The ability to automatically provision and release capabilities in specific situations allows for rapids calling out and scaling in. In terms of provisioning, clients have seemingly countless options to pick from, and they may buy as many as they want, anytime they want.
•
• A metering capability at a level of abstraction appropriate to the type of service is used to automatically control and optimize resource use in cloud computing systems. • (e.g., storage, processing, bandwidth, and active user accounts). When resources are monitored, controlled and reported on, both service providers and service user's profit.

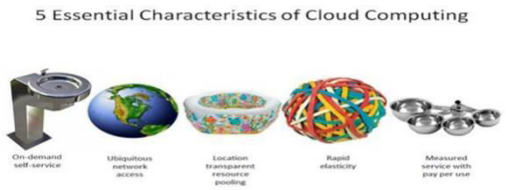

Fig: 1.2 Characteristics of cloud computing

II. RELATED WORKS

The software development process is not complete until a comprehensive literature review has been conducted. Time, cost, and company Traffic Redundancy Elimination must all be calculated before development of the tool can begin; once these requirements are met, it will be possible to choose an appropriate operating system and programming language. Once development of the tool begins, however, programmers require extensive outside assistance. This guidance is available from seasoned programmers, books, and online resources.

The following ideas are necessary for constructing the proposed system.

[1] The kerberos network authentication service (5th version), by C. Neuman, S. Hartman, and K. Raeburn, RFC 4120, 2005.
This document supersedes RFC 1510 as the authoritative reference for the Kerberos protocol and its intended use, as it provides a more thorough and clear explanation of certain aspects of the protocol and its intended use. The goal of this document is to provide a comprehensive, implementable description of the protocol, complete with guidelines for how to send and receive messages and how to fill out fields in those messages.

[2] This is the "OAuth Protocol." [Online]. Find it at http://www.oauth.net/.
To communicate authorization choices across a group of web-enabled applications and APIs, the OAuth 2.0 specification defines a delegation protocol. OAuth has many uses, one of which is the provision of user authentication mechanisms. As a result, many programmers and API providers have made the assumption that OAuth is an authentication protocol in and of itself. Let us restate that for emphasis: OAuth 2.0 is not an authentication protocol.
Because OAuth is embedded within authentication protocols, it's common for developers to mistakenly believe that using OAuth to authenticate users is as easy as interacting with its components and following its flow. Not only does this turn out to be false, but it also poses serious risks to service providers, developers, and end users.
To answer the question of how to construct an authentication and identity API with OAuth 2.0 as the foundation, this article is written for potential identity providers. If you are saying something along the lines of "I have OAuth 2.0, and I need authentication and identity," then you should keep reading.

[3] The "Open ID Protocol." [Online]. Open ID Authentication, which can be found at http://openid.net/, is a method by which an end user can demonstrate that they are the rightful owners of an Identifier. It achieves this without revealing any private information to the Relying Party, including user credentials like passwords or email addresses.
Open ID is a distributed system. There is no need for Relying Parties or Open ID Providers to be authorized or registered with a centralized body. An end user has complete

autonomy over their Open ID Provider of choice and can keep their Identifier even if they switch.
The authentication method is compatible with "AJAX"-style setups, but the protocol itself doesn't necessitate JavaScript or up-to-date browsers. In other words, the user doesn't even have to leave the page they're currently on to provide Identity Proof to the Relying Party.

Open ID Authentication does not necessitate any unusual features of the User-Agent or other client software, as it only makes use of standard HTTP(S) requests and responses. Open ID is independent of cookies or any other similar mechanism used by Relying Parties or Open ID Providers to manage user sessions. Extensions to User-Agents are not required to use the protocol but can facilitate easier interaction with end users.

Additional service types built on top of this protocol to create a framework can address the exchange of profile information or the exchange of other information not covered in this specification. Open ID Authentication's primary goal is to supply a foundational service that allows for free, decentralized, and mobile digital identities for its users.

[4] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization."
Kerberos, since its creation, has become the standard method for deploying centralized authentication services. Over the past few years, LDAP—the Lightweight Directory Access Protocol—has prevailed as the standard for the centralized management of user identities. Both pieces of infrastructure are being used more frequently by businesses to facilitate the administration of decentralized data transmission networks. Over the course of this development, a common authorization framework has not emerged. The vast majority of experts agree that LDAP is the best protocol for storing the kinds of in-depth data that are required to make informed authorization choices. Despite this agreement, a standardized approach to implementing directory-based authorization has not yet emerged. An approach to implementing directory-based authorization using Kerberos's symmetric key management facilities is discussed in this paper. Due to the design of the system, directory compromises are extremely unlikely to compromise the security of the system. The system allows for fine-grained authorization control to be implemented alongside the management benefits of role-based access systems. Authorization in the identity-based model is handled in a service-oriented manner. So, it fits in with and even helps advance the movement toward service-oriented app architectures.
According to [5] "A nonce-based protocol for multiple authentications," published in ACM SIGOPS Operating System Review, volume 26, issue 4, pages 84-89, and 1992. Authors: A. Kehne, J. Schonwalder, and H. Langendorfer.
The Needham and Schroeder protocol is the foundation for MIT's Kerberos authentication service, which was developed as part of Project Athena. To ensure that messages are up-to-date, time stamps based on accurate synchronized clocks are used. To improve upon Kerberos, we introduce a nonce-based protocol with the same capabilities. In the first round of communication, we create a ticket that contains a generic timestamp. The onus of verifying this nonspecific timestamp falls on the creator. As a result, we can get by without using coordinated timepieces. For our protocol to generate a trusted session key, only a small number of messages are required.

III. METHODOLOGY

In order to enable safe access to a remote (cloud) server, we build a new biometric-based authentication system in this paper. In the suggested method, we treat a user's biometric information as a secure credential. From the user's biometric information, we then create a unique identity that is utilized to generate the user's private key. Additionally, we offer a practical method for creating a session key for secure message transmission between two conversing participants utilizing two biometric templates. In other words, the user's private key does not need to be stored anywhere, and the session key is generated secretly.

A.IMPLEMENTATION

Modules Used in Project:

O Data Owner

The data owner uploads their biometric images and associated data to the cloud server in this module. The data owner assigns a digital signature and stores it in the cloud for security purposes, performing identical actions for the following: Publish a biometric image with a digital sign based on the title, description, and list all biometric images that have been uploaded, confirm biometric image

information, and remove biometric image details.

O Cloud Server

A pall is managed by the pall service provider to provide data storage service. And carries out comparable actions as the following with their hand, save all biometric image lines. View every biometric picture line and its information. View all comments on biometric images, View all data holders, drug users, and bushwhackers.

O Users

The Cloud Stoner, who has the authority to access and alter stored Biometric images and their data and who has a significant amount of data to be stored in Cloud servers. If the user is approved, he can access biometric image data and do actions including searching for biometric images, accessing biometric images and their details, and more. Download the biometric image and provide feedback.

IV. EXPERIMENT, RESULTS, AND ANALYSIS

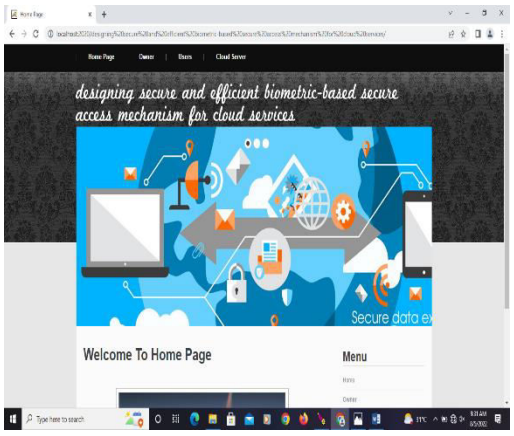

Fig 2: The above screen is the Home page. In this home page user, owner And cloud server exists.

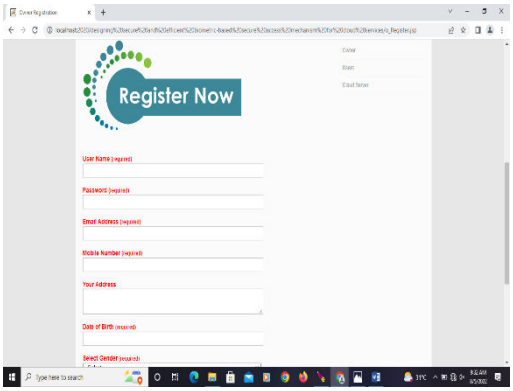

Fig 3: In the above screen the owner can register using fields

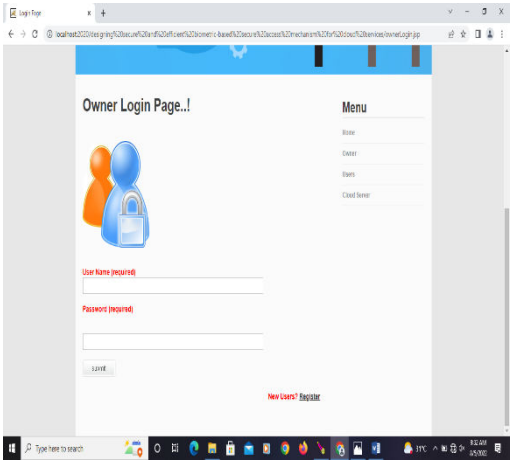

Fig 4: In the above screen the owner can login by using user name and password

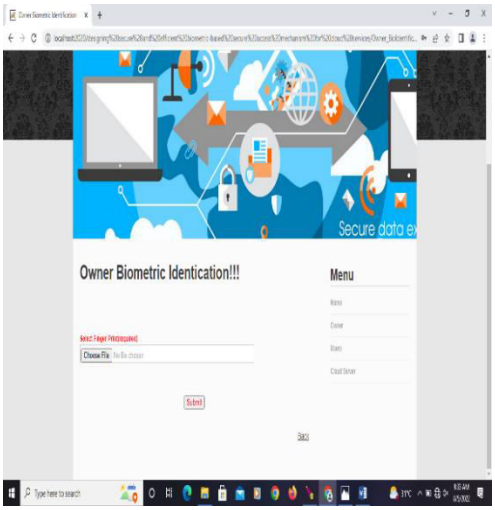

Fig 5: In the above screen owner needs provide biometric image for login if the image is correct then owner can view his actions

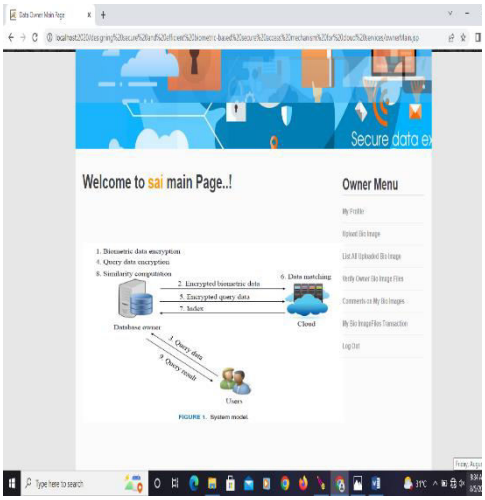

Fig 6: The above screen is the owner main page. He can do actions in this page like view his profile, upload biometric images, verify his biometric images etc….

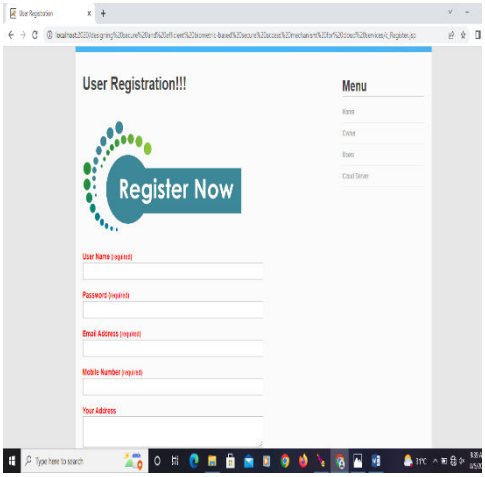

Fig 7: In the above screen the user can register using fields

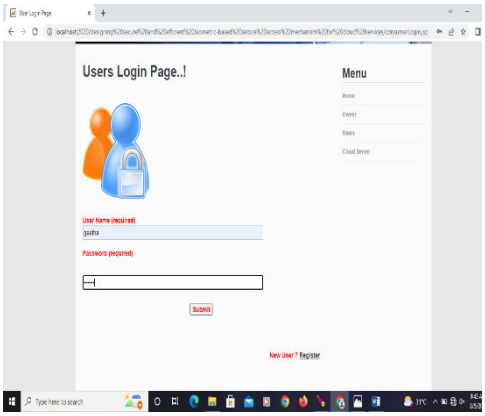

Fig 8: In the above screen the user can login by using user name and password

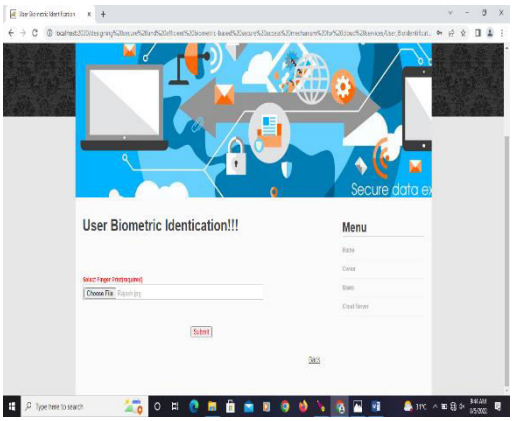

Fig 9: In the above screen user needs provide biometric image for login if the image is correct then user can view his actions

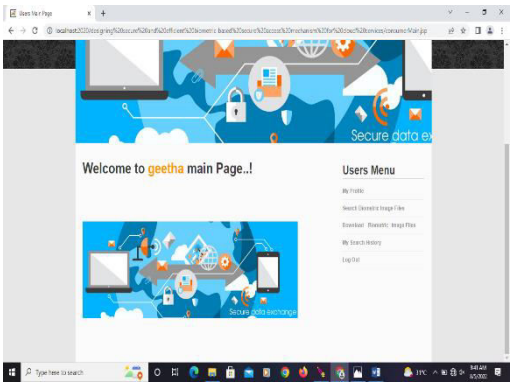

Fig 10: The above screen is the user main page. He can search his biometric image files and download

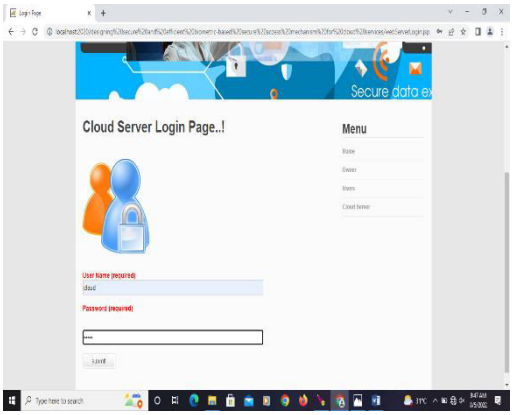

Fig 11: In the above screen the cloud server login by using user name and password

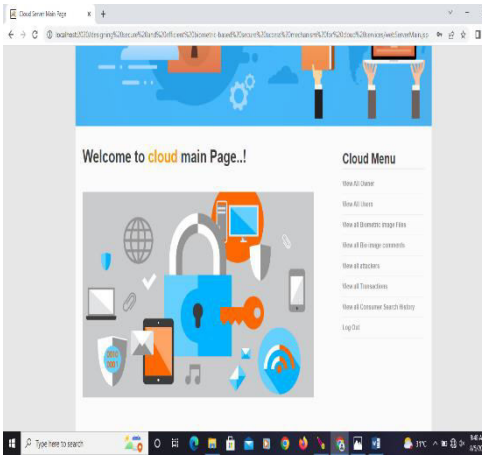

Fig 12: the above screen is the cloud server main page. In this page we can See all users and owners, attackers etc...

V. CONCLUSION AND FUTURE WORK

The growing use of biometrics demonstrates that it offers distinct advantages over traditional password and token-based security systems (e.g., on Android and IOS devices). In this paper, we present an authentication method based on biometrics for users attempting to access services and computing resources from a distance. Our suggested method makes it possible to build a private key from a fingerprint biometric reveal because it is possible to do so with 95.12% accuracy. There is no need to communicate any prior information when using the session key creation method we suggest using two biometric data. Our strategy is more resistant to a number of known attacks when compared to other authentication methods of a similar nature. Future investigation will examine additional.

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 medicaldevices,"inProc.ofIEEEGLOBECOM2010, pp.1-5, 2010.
[10] M. Barni, T. Bianchi, D. Catalano, et al., "Privacy-preservingfingercode 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), 2010IEEE Symposiumon,pp. 239-254, 2010.
[12] D.Evans,Y.Huang,J.Katz,etal.,"Efficientprivacy-preservingbiometric identification," in Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS, 2011.
[13] J.Yuanand S.Yu, "Efficient privacy-preserving biometric identification in cloudcomputing,"inProc.ofIEEEINFOCOM2013, pp.2652-2660, 2013.
[14]Q.Wang,S.Hu,K.Ren,etal."CloudBI:Practical privacy-preserving out sourcing of biometric identification in the cloud," in European Symposium on Research in Computer Security, pp. 186-205, 2015.
[15]Y.Zhu,Z.WangandJ.Wang,"Collusion-resistingsecurenearestneighbor query over encrypted data in cloud," In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on, pp. 1-6, 2016.
[16] S. Pan, S. Yan, and W. Zhu, "Security analysis on privacy-preserving cloud aided biometric identification schemes," in Australasian Conference on Information Security and Privacy, pp. 446-453, 2016.