Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

AN INNOVATIVE BIOMETRIC-BASED SECURE ACCESS MECHANISM IMPLEMENTATION FOR VARIOUS CLOUD-BASED SERVICES

G. Venugopal Associate Professor,Department of CSE,PBR VITS, Kavali.
1, P. Vaishnavi 2, K. Sowmya 3, M. Pavithra Devi 4, M. Sai Pujitha 5 students, Department of CSE, VISVODAYA ENGINEERING COLLEGE, Kavali.

Abstract_ In our data-driven society, the demand for remote data storage and computation services is increasing exponentially, as is the need for secure access to such data and services. We propose a new biometric-based authentication protocol in this paper to provide secure access to a remote (cloud) server. We consider a user's biometric data as a secret credential in the proposed approach. The user's biometric data is then used to generate a unique identity, which is then used to generate the user's private key. Furthermore, we propose a simple method for generating a session key between two communicating parties using two biometric templates for secure message transmission. In other words, there is no need to save the user's private key anywhere, and the session key is generated without any prior information being shared. A thorough Real-Or-Random (ROR) model-based formal security analysis, informal (non-mathematical) security analysis, and formal security verification using the widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool demonstrate that the proposed approach can withstand several known attacks against (passive/active) adversaries. Finally, extensive experiments and a comparative study demonstrate the proposed approach's efficiency and utility..

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

2.1 BLACR: without ttpblacklistable obscure confirmations with reputation Authors: M. H. Au, A. Kapadia, and W. Susilo

Baffling approval can give customers the license to turn crazy since there is no fear of retaliation. As an obstacle, or means to refusal, various designs for mindful mystery feature a (possibly passed on) trusted in untouchable (TTP) with the capacity to recognize or interface misbehaving customers. Starting late, plans, for instance, BLAC and PEREA showed how obscure denial can be practiced without such TTPs—strange customers can be disavowed in case they get into wickedness, yet then nobody can recognize or association such customers cryptographically. Regardless of being the top tier in obscure revocation, these plans license only an essential sort of renouncement signifying 'deny anybody with d or more wicked exercises' or 'repudiate anybody whose joined wrongdoing score is unreasonably high' (where devilish exercises are dispensed a 'reality' score). We present BLACR, which generally impels secretive forswearing in three unique manners: 1) It sets up a first undertaking to summarize reputation based obscure denial, where negative or positive scores can be delegated to strange gatherings over different classes. Laborers can square customers subject to methodologies, which decide a boolean mix of reputations in these orders; 2) We present a weighted expansion, which allows the full scale earnestness score to increment for different wicked exercises by a comparative customer; and, 3) We make an immense improvement in approval times through a strategy we call express way affirmation, which makes reputation based obscure renouncement sensible.

2.2 PERM: Practical reputation based boycotting without TTPS Authors: M. H. Au and A. Kapadia

A couple of customers may get into underhandedness under the front of anonymity by, e.g., harming site pages on Wikipedia or posting revolting comments on YouTube. To thwart such abuse, a few obscure accreditation plans have been proposed that repudiate access for getting into wickedness customers while keeping up their anonymity with the ultimate objective that no trusted in pariah (TTP) is locked in with the denial technique. Starting late we proposed BLACR, a without ttp plot that supports 'reputation based boycotting' - the pro community can score customers' strange gatherings (e.g., incredible versus ill-advised comments) and customers with lacking reputation are denied get to. The critical drawback of BLACR is the direct computational overhead in the size of the reputation list, which grants it to help reputation for only a few thousand customer gatherings in valuable settings. We propose PERM, a disavowal window-based arrangement (wicked exercises must be gotten inside a window of time), which makes count liberated from the size of the reputation list. PERM in this manner supports a considerable number of customer gatherings and makes reputation based boycotting rational for gigantic extension courses of action.

2.3 Constant-size one of a kind k-TAA Authors: M. H. Au, W. Susilo, and Y. Mu

Dynamic k-times obscure confirmation (k-TAA) plans grant people from a social occasion to be affirmed subtly by application providers for a predetermined number of times, where application providers can self-rulingly and logically grant or deny get the opportunity to right to people in their own get-together. In this paper, we fabricate an incredible k-TAA plot with reality complexities of O(log(k)) and a variety, where the check show just requires consistent presence complexities to the detriment of O(k) - estimated open key. We in like manner portray some tradeoff issues between different system characteristics. We detail all the zerodata affirmation of-data shows included and show that our improvement is secure in the discretionary prophet model under the qstrong Diffie–Hellman assumption and qdecisional Diffie–Hellman inversion doubt. We give a proof-of-thought execution, test its display, and show that our arrangement is businesslike.

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

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

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

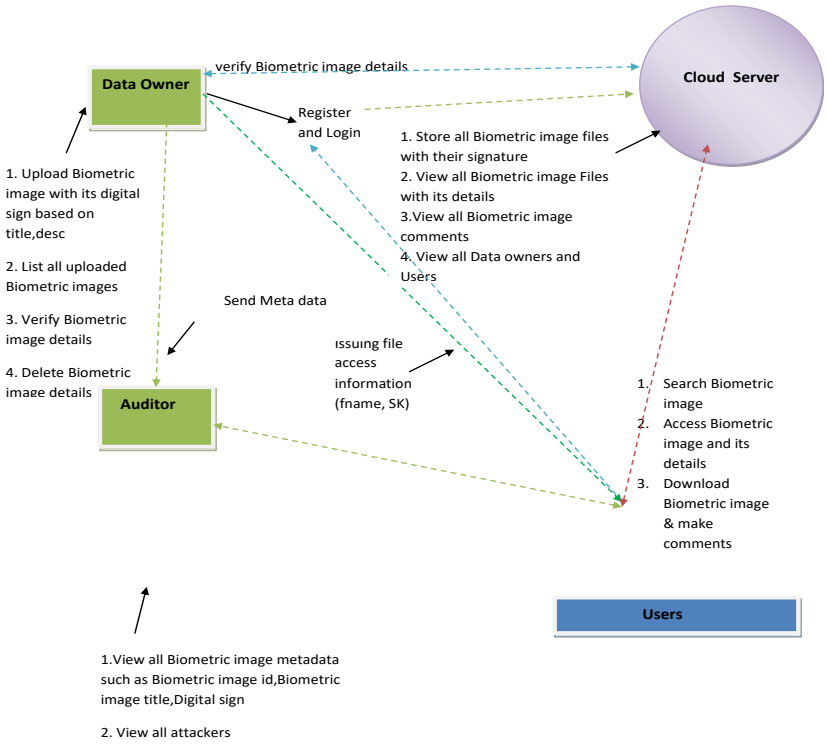


Fig: 1. System Model

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

4.RESULTS AND DISCUSSIONS

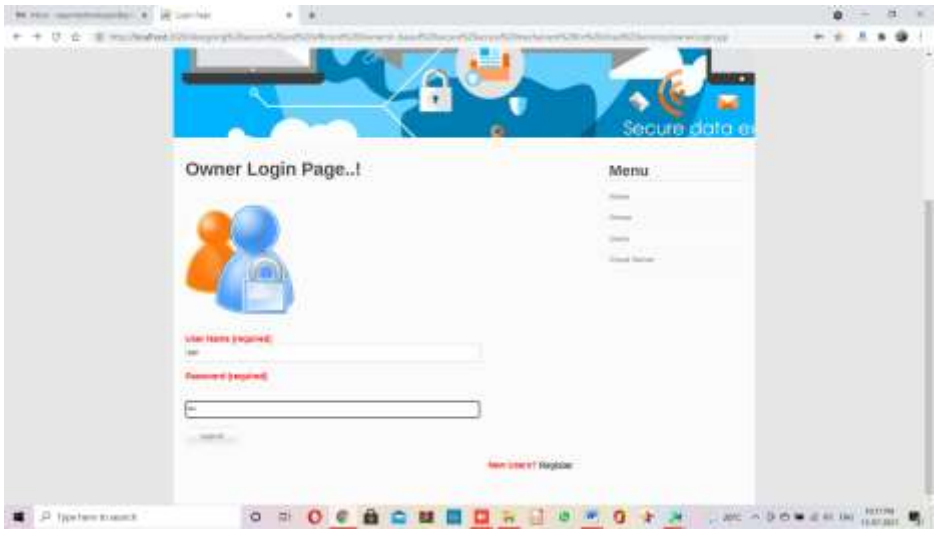
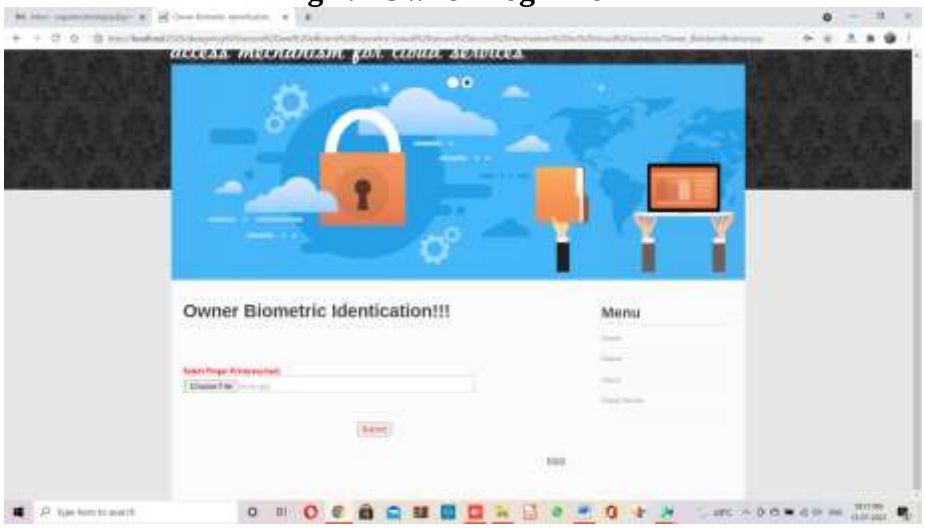


Fig 4.1 Owner Login Form



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

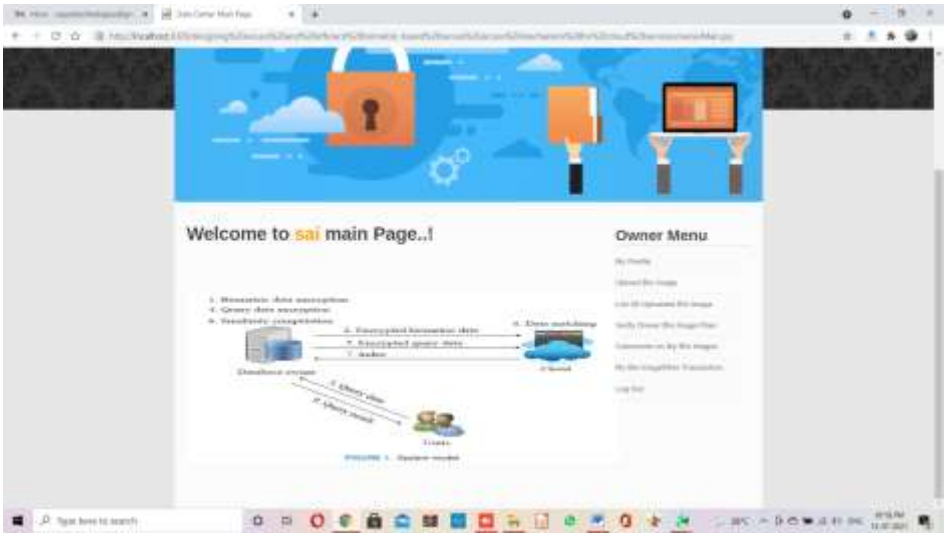


Fig 4.3 owner main page

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.