International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 2, Mar- Apr 2024

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

AVISPA TOOL: A SECURITY ANALYSIS TOOL FOR SECURE CRYPTO BIOMETRIC SYSTEM

Dr D J Samatha Naidu[1], K.Venkata Ramya [2] , D. Mahaboob Basha[3]

MCA Department, Annamacharya PG College of Computer Studies, Rajampet

----------**********----------

Abstract:

Biometric has its unique advantages over conventional password and token-based security system. As evidenced by its increased adoption.Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which however brings potential threats to users' privacy. In this project to propose an efficient and privacy-preserving biometric identification outsourcing scheme. Specifically, the biometric data is encrypted and outsourced to the cloud server. To execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over the encrypted database and returns the result to the database owner. A thorough security analysis indicates the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with previous protocols, experimental results show the proposed scheme achieves a better performance in both preparation and identification procedures.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 reveal, as it is possible to generate to 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.

Keywords —Authentication, biometric-based security, cloud service access, session key.

----------**********----------

I. INTRODUCTION

Cloud services are 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 going challenges, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos, Oauth and OpenID. 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

 ©IJSRED:All Rights are Reserved

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.*, Althobaiti*et al*, Xue *et al.*, Turkanovic*et al.*, Park *et al.*, Dhillon and Kalra, Kaul and Awasthi and Kang *et al.* – 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.

In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometric based message authenticator is also generated for message authenticity purpose.

We summarize the key contributions/benefits related to the proposed approach as below.

1. An effective way to transmit the user's biometric data through the unsecured network channels to an authentication server is presented.
2. We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere.
3. We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server.
4. We introduce a novel way to generate session keys.
5. In traditional authentication protocol, each entity requires some preloaded information; thus, incurring some overhead. We introduce a new mechanism to avoid the need for secret pre-loaded information.
6. A message authentication mechanism, as an alternative to the existing message authentication protocol (i.e., Message authentication code (MAC)), is introduced.

In the next section, we will review existing biometric based authentication schemes, prior to presenting the proposed biometric-based authentication approach in Section III. We then evaluate the performance and security of the proposed protocol in Sections IV and V, respectively. Specifically, we demonstrate that the protocol is secure in the presence of a Dolev-Yao (DY) adversary. Then, a comparative study is presented in Section VI. Finally, Section VII concludes the paper.

I. EXITING SYSTEM

One example of an existing biometric-based secure access mechanism is the implementation of fingerprint recognition technology in smartphones and other devices. Many modern smartphones feature fingerprint sensors embedded within the device's home button or on the rear panel. These sensors capture and analyse the unique patterns of an individual's fingerprint to authenticate their identity.

Upon setting up the device, users are prompted to enroll their fingerprints by placing their finger on the sensor multiple times to capture various angles and details of the fingerprint. This enrolment process creates a template or "fingerprint signature" unique to each user, which is securely stored within the device's hardware or software.

 ©IJSRED: All Rights are Reserved

During the authentication process, when a user attempts to unlock the device or access sensitive information, they are required to place their finger on the fingerprint sensor. The sensor then compares the captured fingerprint with the stored template to verify the user's identity. If the fingerprint matches the template within an acceptable margin of error, the device grants access to the user.

Disadvantages

- The system doesn't implement Biometric Identification Scheme.
- There is no an efficient privacy preserving encryption techniques in this system.

I. PROPOSED SYSTEM

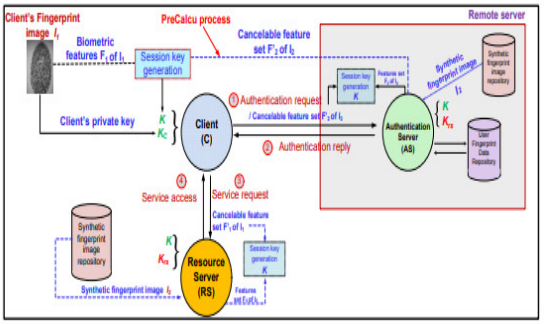
The proposed system examines the biometric identification scheme and shows its insufficiencies and security weakness under the proposed level-3 attack.

The system presents a novel efficient and privacy-preserving biometric identification scheme. The detailed security analysis shows that the proposed scheme can achieve a required level of privacy protection.

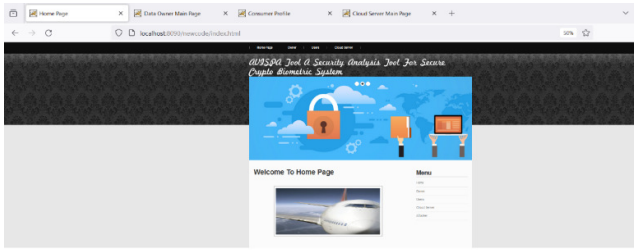
Advantages

- An efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users.
- Attackers can only observe the encrypted data stored in the cloud. In order to avoid, the well-known cipher text-only attacks.

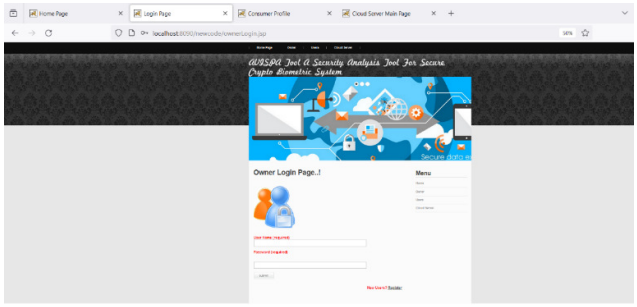
II. SYSTEM ARCHITECTURE



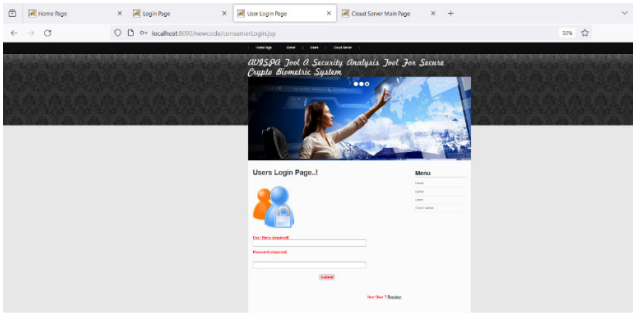
III. SAMPLE SCREENS



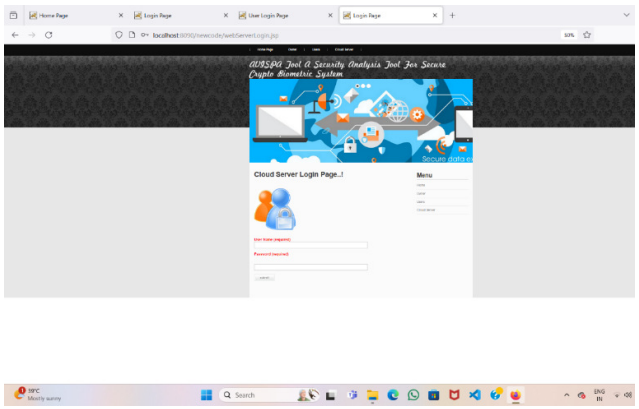
SCREEN 1 HOME PAGE



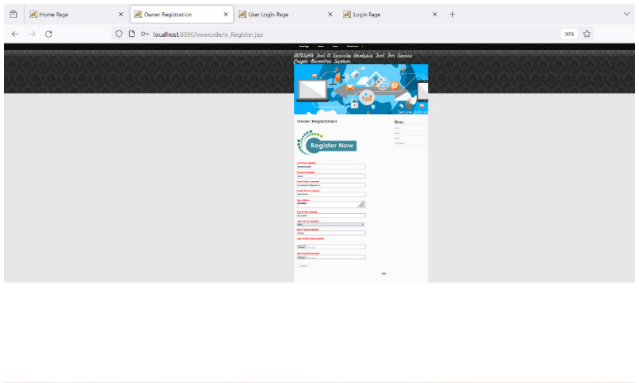
SCREEN 2 OWNER LOGIN PAGE



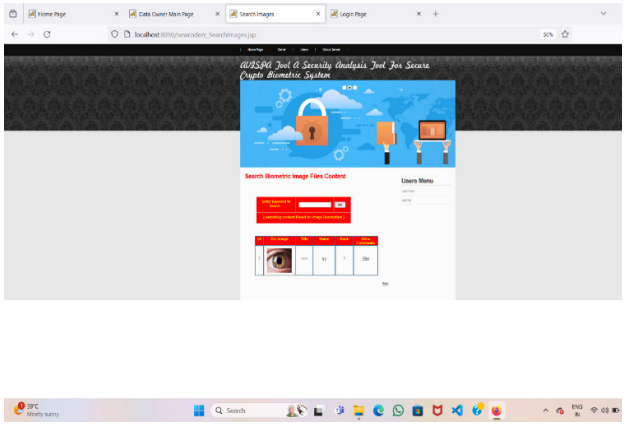
SCREEN 3 USER LOGIN PAGE



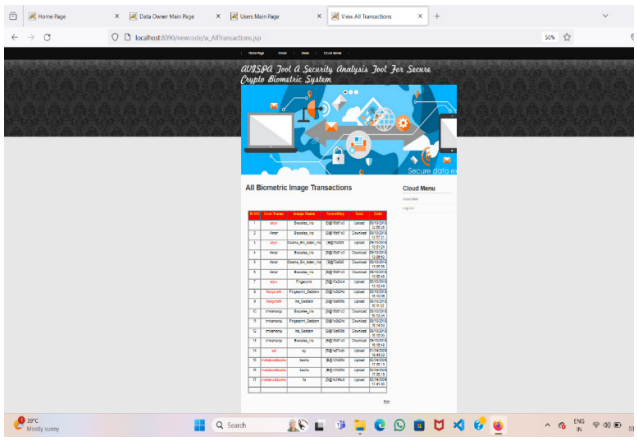
SCREEN 4 CLOUD SERVER LOGIN PAGE



SCREEN 5 REGISTRATION PAGE



SCREEN 6 SERACHING BIOMETRIC IMAGE FILE CONTENT



SCREEN 7 VIEW ALL BIOMETRIC IMAGE TRANSACTION

CONCLUSION

In this project we study how to provide an efficient and privacy preserving biometric identification outsourcing scheme. As online transactions help people to easily complete their tasks, but it has less security and getting hacked. Thus, we propose a novel efficient and privacy preserving biometric identification scheme that provides a lower computational cost in both preparation and identification procedures. The detailed analysis shows it can resist the potential attacks. Besides, through performance evaluations, we further demonstrated the proposed scheme meets the efficiency need well.

ACKNOWLEDGMENT

This work was supported by the China National Basic Research Program (973 Program, No. 2015CB352400), NSFC under grant U1401258, NSCF under grant No. 61572488. This research was also supported in part by grants R-252-000-473-133 and R-252- 000-473-750 from the National University of Singapore. We also thank Yipeng Wu for sourcing the data in this study.

REFERENCES

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th

ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

2. G. Ateniese, R.D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. 4th International Conference on Security and Privacy in Communication Networks, 2008

3. F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.

4. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MRPPDP: Multiple-Replica Provable Data Possession," Proc. 28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.

5. H. Shacham and B. Waters, "Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.

6. C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

7. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.

8. K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Challenges, Methods and opportunities," World Wide The project proposes, vol. 15, no. 4, pp. 409-428, 2012.

9. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

 ©IJSRED: All Rights are Reserved