A REVIEW ON DESIGNING SECURE AND EFFICIENT BIOMETRIC-BASED SECURE ACCESS MECHANISM FOR CLOUD SERVICES

ARCHANA DUGGIRALA [1] Dr. SARATH DUGGIRALA [2]

[1] C.S.E Student, Dept of C.S.E, RK College Of Engineering, Kethanakonda, A.P., India

[2] Assistant Professor, Dept of C.S.E, RK College Of Engineering, Kethanakonda, A.P., India

ABSTRACT

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 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. A detailed Real-Or- Random (ROR) model based formal security analysis, informal (non-mathematical) security analysis and also formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool reveal that the proposed approach can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach.

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

INTRODUCTION

Cloud services are a 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 ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [2] and OpenID [3] (see [1], [4]– [12]). 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 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. [13], Althobaiti et al. [14], Xue et al. [15], Turkanovic et al. [16], Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19] and Kang et al. [20] – 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.

LITERATURE SURVEY

Due to the widespread popularity of Internet-enabled devices, Industrial Internet of Things (IIoT) becomes popular in recent years. However, as the smart devices share the information with each other using an open channel, i.e., Internet, so security and privacy of the shared information remains a paramount concern. There exist some solutions in the literature for preserving security and privacy in IIoT environment. However, due to their heavy computation and communication overheads, these solutions may not be applicable

to wide category of applications in IIoT environment. Hence, in this paper, we propose a new biometric-based privacy preserving user authentication (BP2UA) scheme for cloud-based IIoT deployment. BP2UA consists of strong authentication between users and smart devices using preestablished key agreement between smart devices and the gateway node. The formal security analysis of BP2UA using the well-known real-or-random model is provided to prove its session key security. Moreover, an informal security analysis of BP2UA is also given to show its robustness against various types of known attacks. The computation and communication costs of BP2UA in comparison to the other existing schemes of its category demonstrate its effectiveness in the IIoT environment. Finally, the practical demonstration of BP2UA is also done using the NS2 simulation.

Biometric systems are increasingly replacing traditional password- and token-based authentication systems. Security and recognition accuracy are the two most important aspects to consider in designing a biometric system. In this paper, a comprehensive review is presented to shed light on the latest developments in the study of fingerprint-based biometrics covering these two aspects with a view to improving system security and recognition accuracy. Based on a thorough analysis and discussion, limitations of existing research work are outlined and suggestions for future work are provided. It is shown in the paper that researchers continue to face challenges in tackling the two most critical attacks to biometric systems, namely, attacks to the user interface and template databases. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is a hot research topic currently, as well as in the foreseeable future. Moreover, recognition accuracy under non-ideal conditions is more likely to be unsatisfactory and thus needs particular attention in biometric system design. Related challenges and current research trends are also outlined in this paper.

EXISTING SYSTEM

A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [2] and OpenID [3] (see [1], [4]– [12]). 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 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. [13], Althobaiti et al. [14], Xue et al. [15], Turkanovic et al. [16], Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19] and Kang et al. [20] – 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.

Disadvantages:

1.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.

2. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server.

PROPOSED SYSTEM:

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 biometricbased 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.

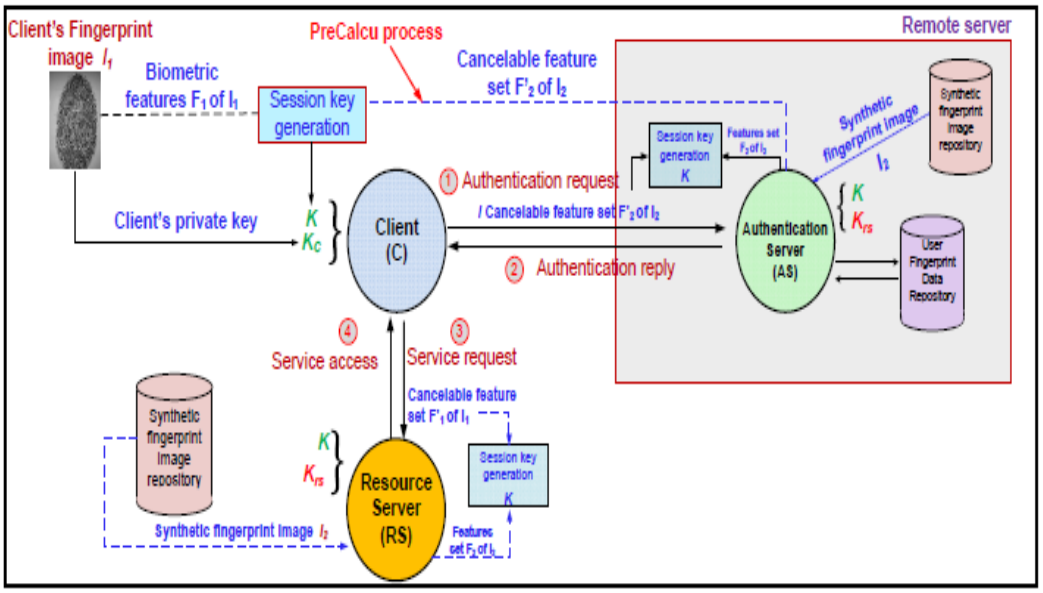
3) We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server.

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.

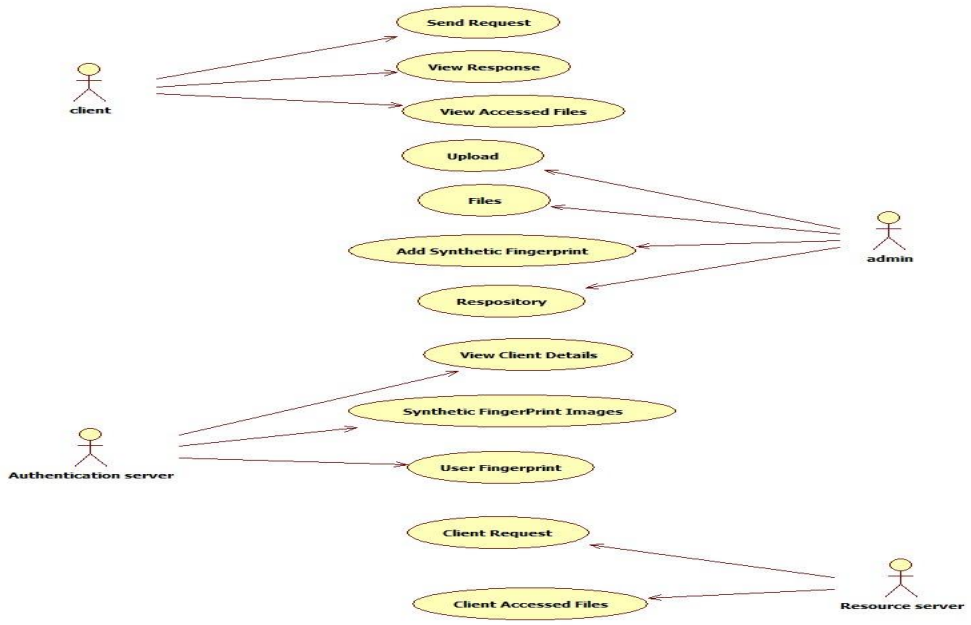
6) A message authentication mechanism, as an alternative to the existing message authentication protocols (i.e., Message Authentication Code (MAC)), is introduced.

SYSTEM ARCHITECTURE



USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



MODULE DESIGN

1. CLIENT

2. AUTHENTICATION SERVER

3. ADMIN

4. RESOURCE SERVER

1) CLIENT

Client has to register into application with basic details and he can able to login with username ,password and with fingerprint. Client can able sent request to the resource server. After sending the request he can get the response from the resource server.after getting the response from the server he can able view the file in the cloud.He can able to see all permission of files.

2) AUTHENTICATION SERVER.

Authentication Server need to login with username and password. After login he can able to view client details and authorize . Authentication server can able to view synthetic finger print images. Server can able to user client images.

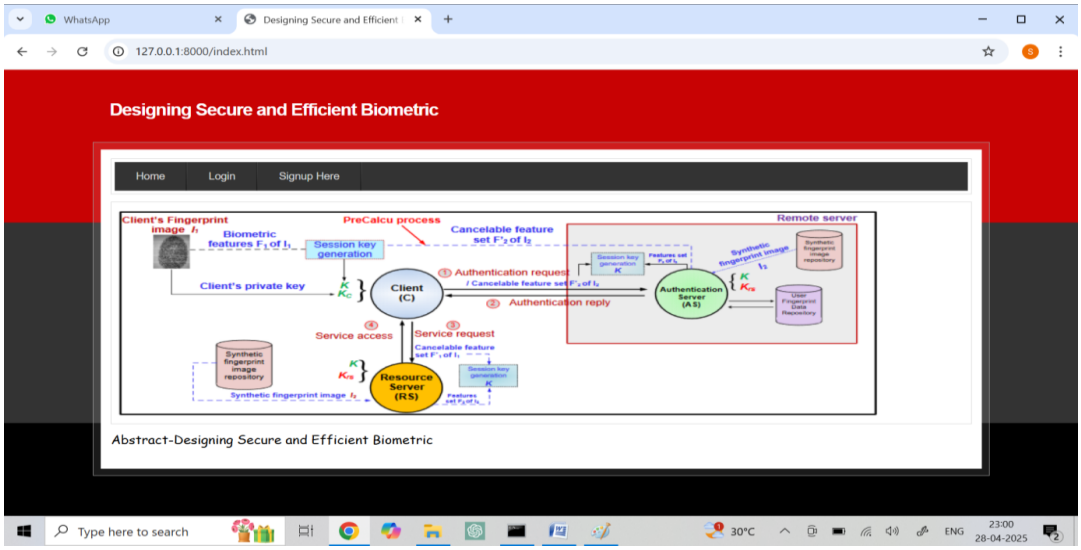
3) ADMIN

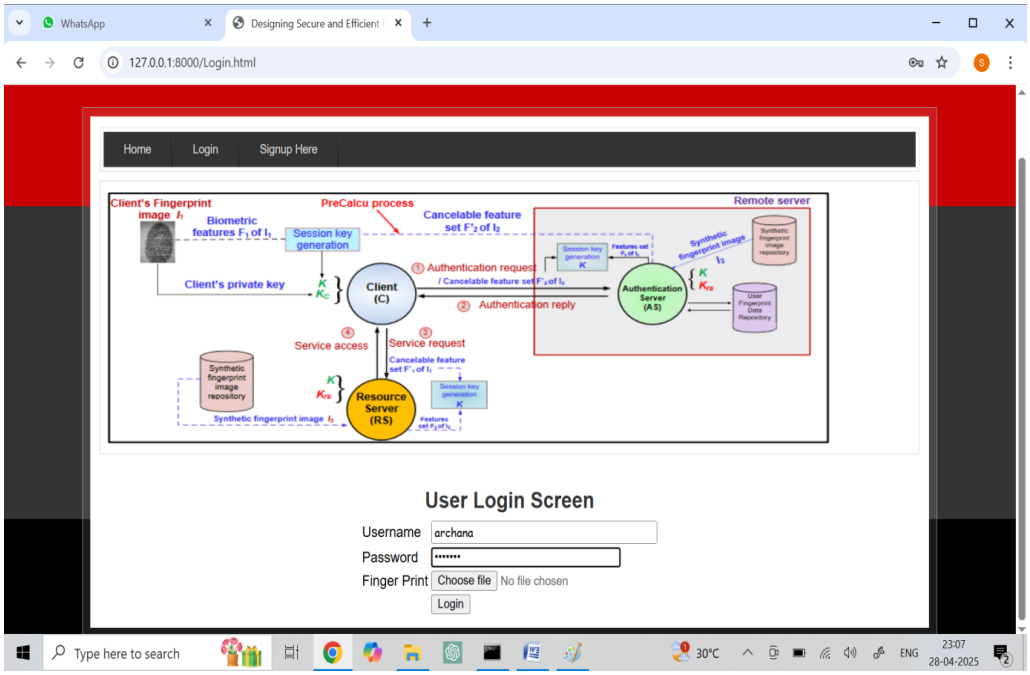
Admin need to login with basic username and password. After login he can able to upload files those are useful to the user. He can able to view all uploaded files. Admin can able to add synthetic fingerprint images.Admin can able to view the data in the repository.

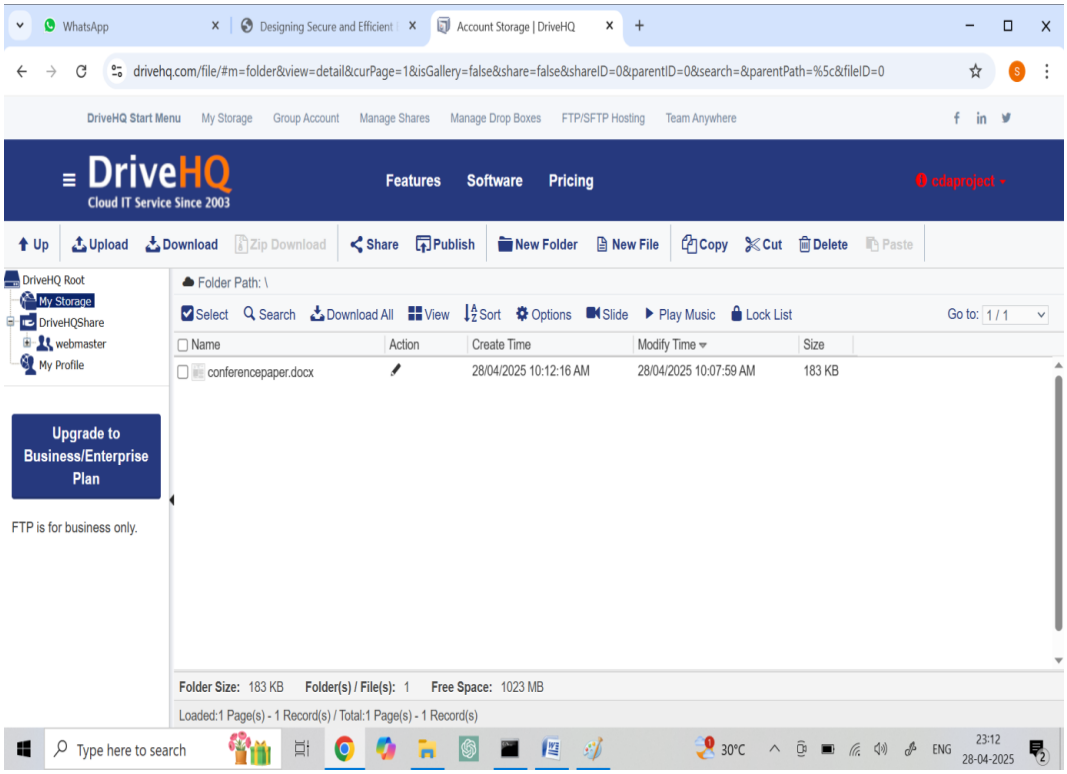
4) RESOURCE SERVER

Resource server need to login into the application using username and password. After login resource server he can able to view all client requests as well as he can able view all users access rights of files.

SCREENSHOTS







CONCLUSION

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced 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 reveals, as it is possible to generate 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. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks. Future research includes exploring other biometric traits and also multi-modal biometrics for other sensitive applications (e.g., in national security matters).

REFERENCES

[1] C. Neuman, S. Hartman, and K. Raeburn, "The Kerberos network authentication service (V5)," *RFC 4120*, 2005.

[2] "OAuth Protocol." [Online]. Available: http://www.oauth.net/

[3] “OpenID Protocol.” [Online]. Available: http://openid.net/

[4] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” in *Proc. AFS and Kerberos Best Practices Workshop*, June 2006.

[5] A. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” *ACM SIGOPS Oper. Syst. Rev.*, vol. 26, no. 4, pp. 84–89, 1992.

[6] B. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” *Oper. Syst. Rev.*, vol. 27, no. 2, pp. 10–14, 1993.

[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon: End-to-end authorisation support for resource-deprived environments,” *IET Inf. Secur.*, vol. 6, no. 2, pp. 93–101, 2012.

[8] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient security mechanisms for large-scale distributed sensor networks,” presented at the *11th ACM Conf. Computer and Communications Security*, Washington D.C., USA, Oct. 2003, pp. 62–72.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS: Security protocols for sensor networks,” *ACM Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, 2002.

[10] P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” *Comput. Commun.*, vol. 17, no. 7, pp. 501–518, 1994.