International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services

Mr. Mohammed Afzal, Asst.Professor*, R. Chaithanya**, M. Supriya***, R. Greeshma****
*(CSE Department, Sphoorthy Engineering College, Nadergul
Email: mdafzal.aiml@gmail.com)
**(CSE Department, Sphoorthy Engineering College, Nadergul
Email : chaithanyareddy293@gmail.com)
***(CSE Departement, Sphoorthy Engineering College, Nadergul
Email :maddisupriya37@gmail.com)
****(CSE Department, Sphoorthy Engineering College, Nadergul
Email: ramidigreeshmareddy@gmail.com)

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.

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

I. 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. Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, (mis)used to which can be stolen and gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a few cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. 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 enrol the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new 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.

II. LITERATURE SURVEY

we have surveyed that existing project and finally thought of making necessary modification for getting the latest edition

Existing System

A number of authentication mechanisms have been proposed in the literature 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 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. 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.

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 biometric based message authenticator is also generated for message authenticity purpose.

III. IMPLEMENTATION

From a captured user's fingerprint image, we extract all minutiae points. In order to increase the accuracy in feature extraction, we first align the fingerprint image. From this aligned fingerprint image, we select the consistent region. The consistent region can be defined as the fingerprint region, which has a high chance of appearance in any captured fingerprint image. We select this consistent region to extract the minutiae points. To select a set of minutiae points from the consistent region, we propose to use a horizontal segment. Horizontal segment is a small area of the consistent region, which has the highest number of minutiae points. We select these minutiae points to generate a Trellis diagram of the convolution coding [39] and finally, a codeword from it. The details process of codeword generation is discussed in [40]. Let’s refer to this codeword as BioCode, which can then be used to generate a private key KC as KC = H(BioCode ./ Kr), where Kr is a random number generated by C’s application, H represents a standard hash function (e.g., Secure Hash Algorithm (SHA-1) [41]) and ./ represents a one-way transformation of two input parameters that is significantly easier to compute in forward direction but not in the backward direction [42]. One can also use SHA-256 [41] to achieve high security in the proposed scheme. We use the codeword in order to generate the cryptographic keys. For this purpose, the implementation of the codeword generation can be obtained at https://github.com/ gauranggithun/BioKAP.git. Next, we define the security mechanism.

An overview of BioCAP is shown in Fig. 1, which comprises three entities. These entities are client(s) (C), authentication server(s) (AS) and some resource server (RS). AS contains a database of users’ registered data, while AS generates RS’s private key during the deployment phase and it is shared between AS and RS. In addition, both AS and RS include a large repository of a similar set of synthetic fingerprint images. Some synthetic fingerprint databases, such as some publicly available databases, are used in the proposed approach. When C wishes to access a service from RS, C first sends an authentication request to AS. AS verifies C’s request and sends a reply message to C upon successful verification. Once C obtains the authentication reply message, C sends a service request to RS for getting the access. RS then verifies the service request. If the service request is verified successfully, RS sends a reply to C. C and RS mutually authenticate each other. A session key between C and AS, and C and RS are used for subsequent secure message communications. Further, the message authenticity is controlled by a message authenticator. BioCAP has two key processes, namely: user registration and user authentication. The user registration requires private key generation, whereas user authentication requires generation of the session key and the message authenticator. BioCAP provides a provision to rollover the private key of a user. In addition, BioCAP is secure, computationally less expensive, and overcomes the inherent weaknesses of biometric verification. Moreover, BioCAP does not need pre-shared keys, and provides smooth mutual authentication mechanism and demands less number of keys to be managed from application and user point of view.

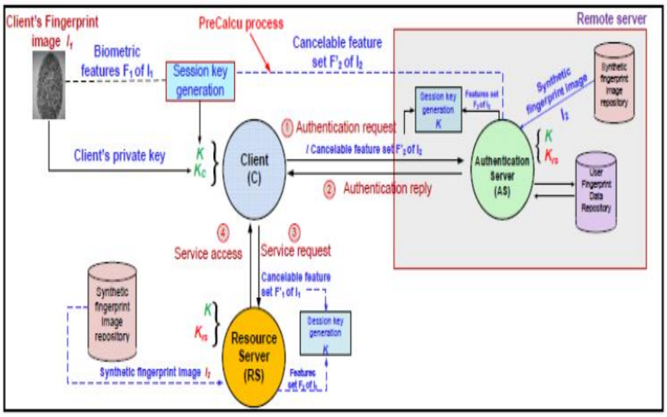
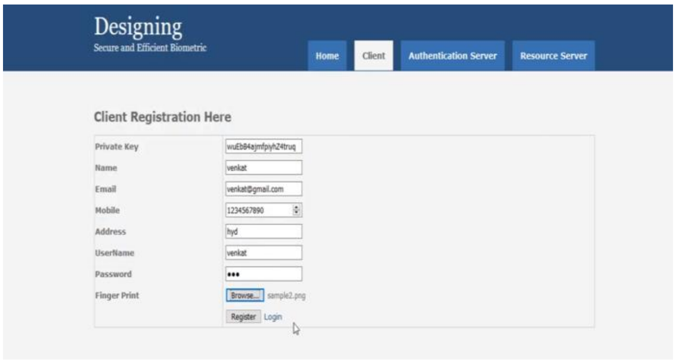

Client's Fingerprint image I_1
PreCalcu process
Remote server
Biometric features F_1 of I_1
Session key generation
Cancelable feature set F'_2 of I_2
Session key generation K
Features set F_2 of I_2
Synthetic fingerprint image I_2
Synthetic fingerprint image repository
① Authentication request / Cancelable feature set F'_2 of I_2
Client's private key
K K_c
Client (C)
Authentication Server (AS)
K K_{rs}
② Authentication reply
User Fingerprint Data Repository
④ Service access
③ Service request
Cancelable feature set F'_1 of I_1
Synthetic fingerprint image repository
K K_{rs}
Resource Server (RS)
Session key generation K
Synthetic fingerprint image I_2
Features set F_2 of I_2

Fig:1

IV. RESULTS

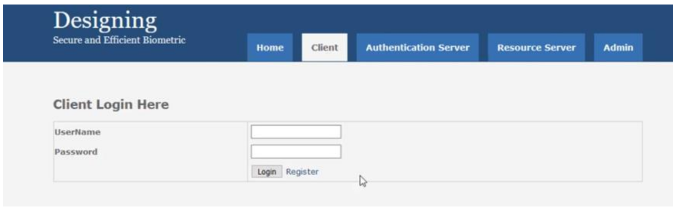
Client registration



Client Registration Here

Private Key	wuEb84ajmfpiyhZ4truq
Name	venkat
Email	venkat@gmail.com
Mobile	1234567890
Address	hyd
UserName	venkat
Password	•••
Finger Print	Browse... sample2.png
	Register Login

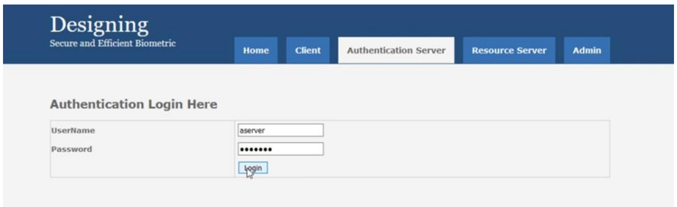
Client login



Client Login Here

UserName	
Password	
	Login Register

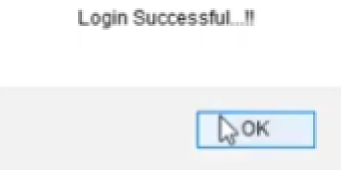
Authentication login



Authentication Login Here

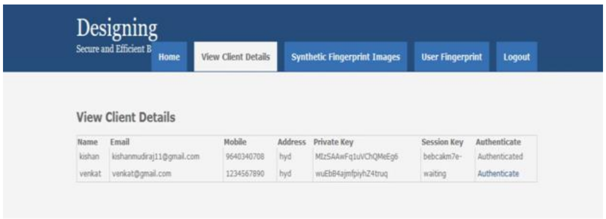
UserName	aserver
Password	•••••••
	Login

Login successful



Login Successful...!!

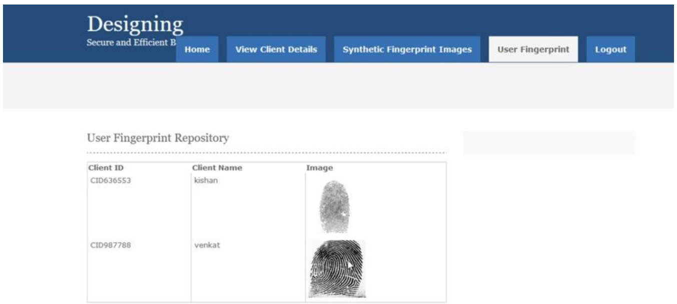
View client details



View Client Details

Name	Email	Mobile	Address	Private Key	Session Key	Authenticate
kishan	kishanmudiraj11@gmail.com	9640340708	hyd	MIzSAAwFq1uVChQMeEg6	bebcakm7e-	Authenticated
venkat	venkat@gmail.com	1234567890	hyd	wuEbB4ajmfpiyhZ4truq	waiting	Authenticate

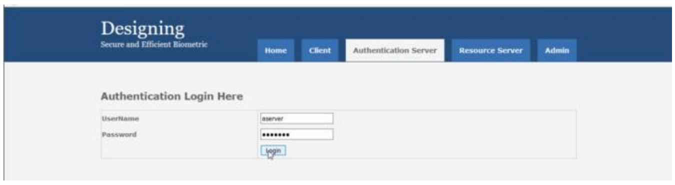
User fingerprint images



User Fingerprint Repository

Client ID	Client Name	Image
CID636553	kishan	
CID987788	venkat	

Admin Login

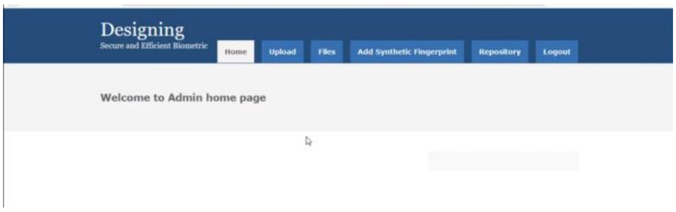


Authentication Login Here

UserName: aserver

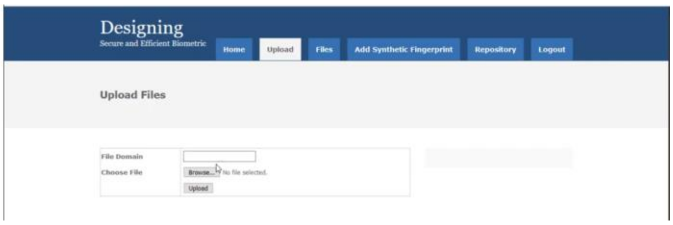
Password: •••••••

Admin Home Page



Welcome to Admin home page

Upload Files

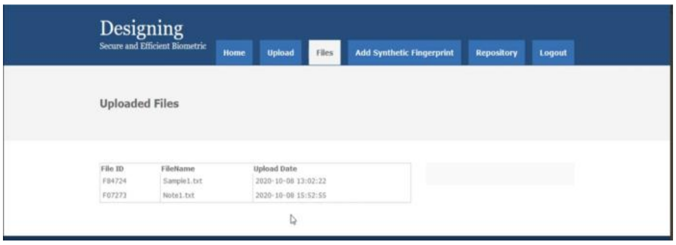


Upload Files

File Domain:

Choose File: No file selected.

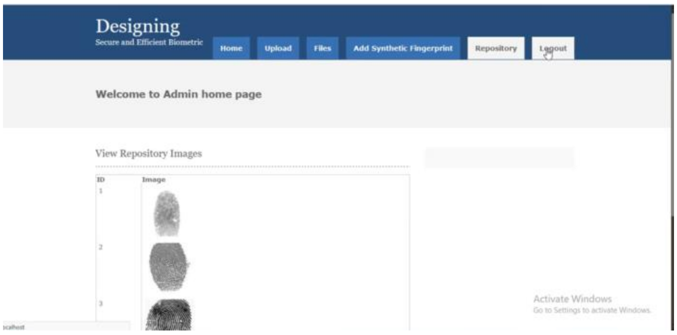
View Files



Uploaded Files

File ID	FileName	Upload Date
F84724	Sample1.txt	2020-10-08 13:02:22
F07273	Note1.txt	2020-10-08 15:52:55

Repository



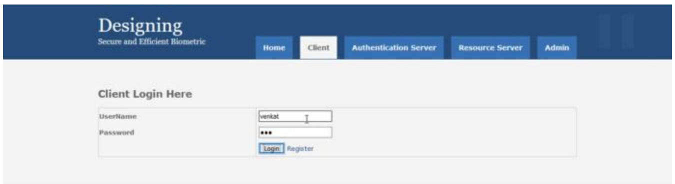
Designing
Secure and Efficient Biometric
Home
Upload
Files
Add Synthetic Fingerprint
Repository
Logout
Activate Windows
Go to Settings to activate Windows.
calhost

Welcome to Admin home page

View Repository Images

ID	Image
1	
2	
3	

User Login

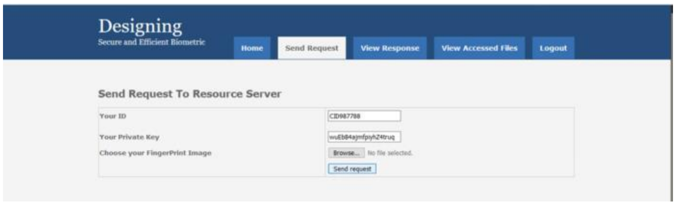


Client Login Here

UserName: venkat

Password: •••

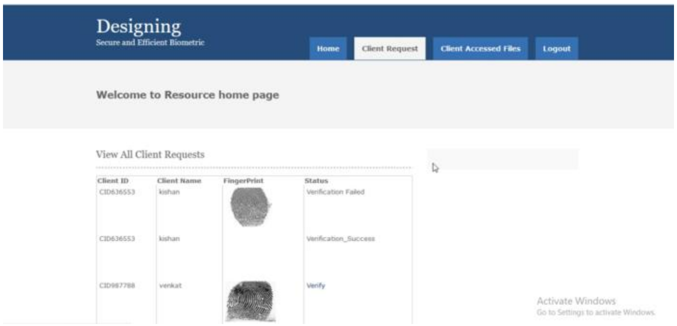
Send Request



Send Request To Resource Server

Your ID	CID987788
Your Private Key	wuEb84ajmfpyhZ4truq
Choose your FingerPrint Image	No file selected.

Client Request

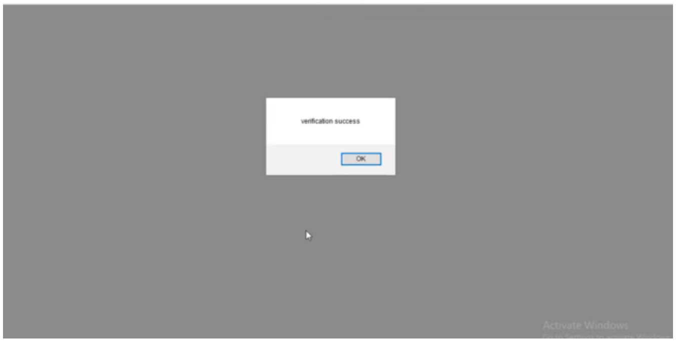


Welcome to Resource home page

View All Client Requests

Client ID	Client Name	FingerPrint	Status
CID636553	kishan		Verification Failed
CID636553	kishan		Verification_Success
CID987788	venkat		Verify

Verifications



verification success

CONCLUSIONS

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 reveal, 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 multi-modal biometrics for other sensitive applications (e.g., in national security matters).

V. REFERENCES

[1] C. Neuman, S. Hartman, 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," 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 Operating System Review, 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 : endto-end authorisation support for resource-deprived environments," IET Information Security, 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," Washington D.C., USA, October 2003, pp. 62–72.