CLOUD BASED BIOMETRIC SECURITY FOR ORGANISATIONS

# Abhinaya R1, Abitha C2, Priyanka B3

\*1Anna University, CSE, Panimalar Engineering College, Chennai, Tamil Nadu, India

\*2Anna University, CSE, Panimalar Engineering College, Chennai, Tamil Nadu, India

\*3Anna University, CSE, Panimalar Engineering College, Chennai, Tamil Nadu, India

(Salini R , Department of CSE Engineering, Panimalar engineering college , Chennai ,Tamil Nadu

,India)

# ABSTRACT (Font-Cambria, Bold, Font Size -12)

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. 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

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 Automate File sharing among multiple Clients is not secure. 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. 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.

# METHODOLOGY

***Existing system***

In existing system uploading and sharing file among multiple client user in cloud environment is very hard to perform and there is no proper authentication among the cloud user and to the cloud server. Hence the file that uploaded on the cloud would not be secure as there is a lot of security problem that related to the cloud storage. 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.

***Proposed system***

In Proposed system, we introduced secure and efficient ﬁle storage and sharing cloud environment using Remote cloud. Mutual authentication is very important between two target device as the user and to the cloud server as mutual authentication makes the server to trust the cloud storage where cloud owner can store the data and from server end, server will verify the user credential to provide any service to that particular user. Cloud contains the encrypted information along with the parameter related to that file. If any user request to the cloud server with some attribute. Based on the attribute cloud will redirect all the related file to the user in order to decrypt the file user need the key for that file for that user request to RSA and DSE(Key Generation Centre) with the file attributes.

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 , 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 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 misused 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.

Therefore, in this paper we seek to design a secure and efficient authentication protocol.

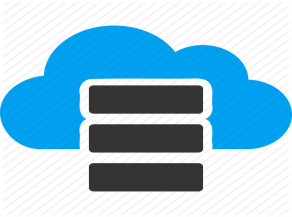
Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information. In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, 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 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.



***Advantage:***

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption.

re)



KGC (Key

Generation Cent

Server Key

User

Fingerprint

Owner Registration

and Mutual Authentication

Service request

User Registration

and Mutual Authentication

File Download

Upload File

Cloud User as Data

Consumer

Key Request to Encrypt

Session key

Access private

key



**BLOCK DIAGRAM DESCRIPTION:**



|  |  |  |
| --- | --- | --- |
| Cloud User as Data Owner |  | |
|  | Fingerprint |
|  |
|  | |

# MODULES AND SPECIFICATIONS

* Cloud Owner and User Registration & Key Generation
* Remote Server Authentication between Devices
* Cloud Owner Upload File to Remote Cloud Server
* Cloud User Decrypt and Download file

1. Cloud Owner and User Registration & Key Generation

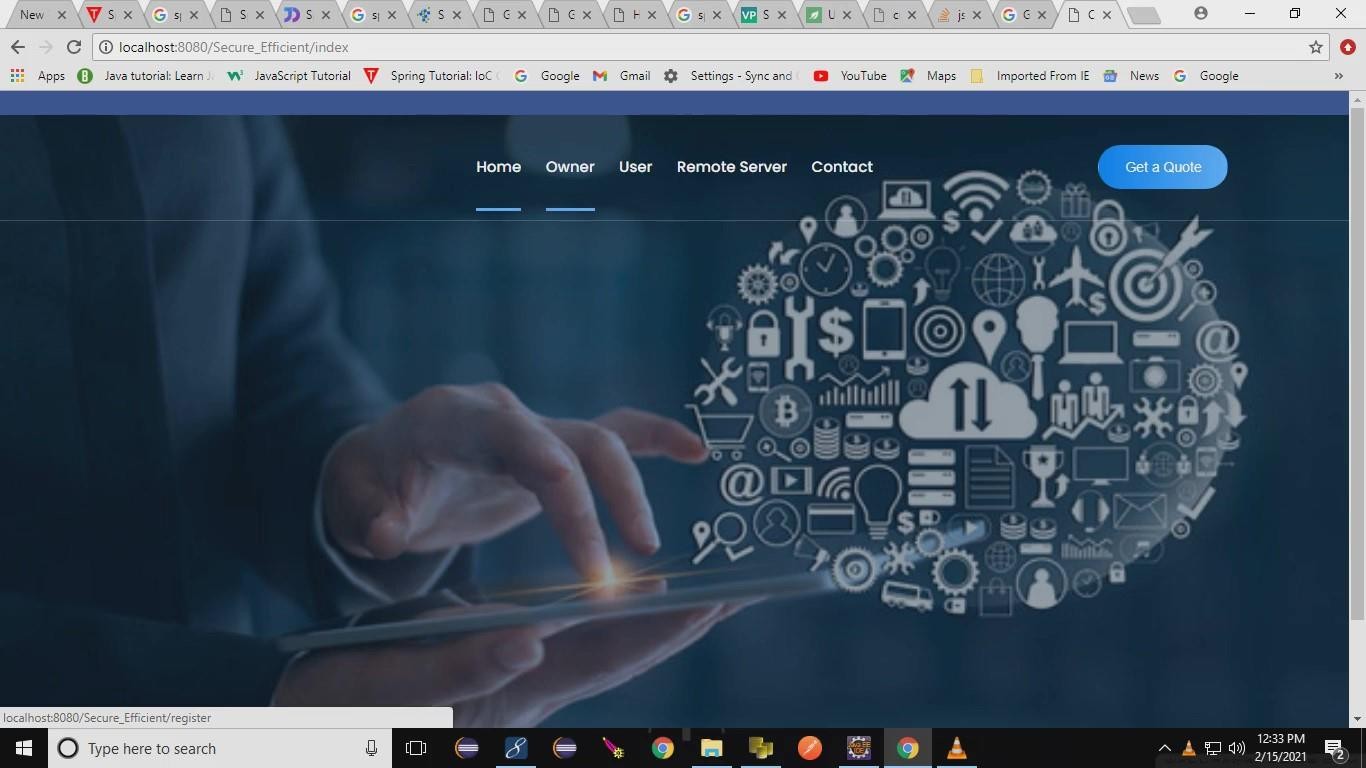
Initially user need to create a account in the cloud sever by providing all the necessary information related to the user like email id, mobile number, age name, password and Cloud Owner a biometric ﬁngerprint then server will generate a unique identity for that Owner and User. Once Owner And User successfully register then user request to Key Generation centre to provide the keys to user by providing the unique id that was generated by the server. User can access the Cloud data only if he registers their name in key generation centre.

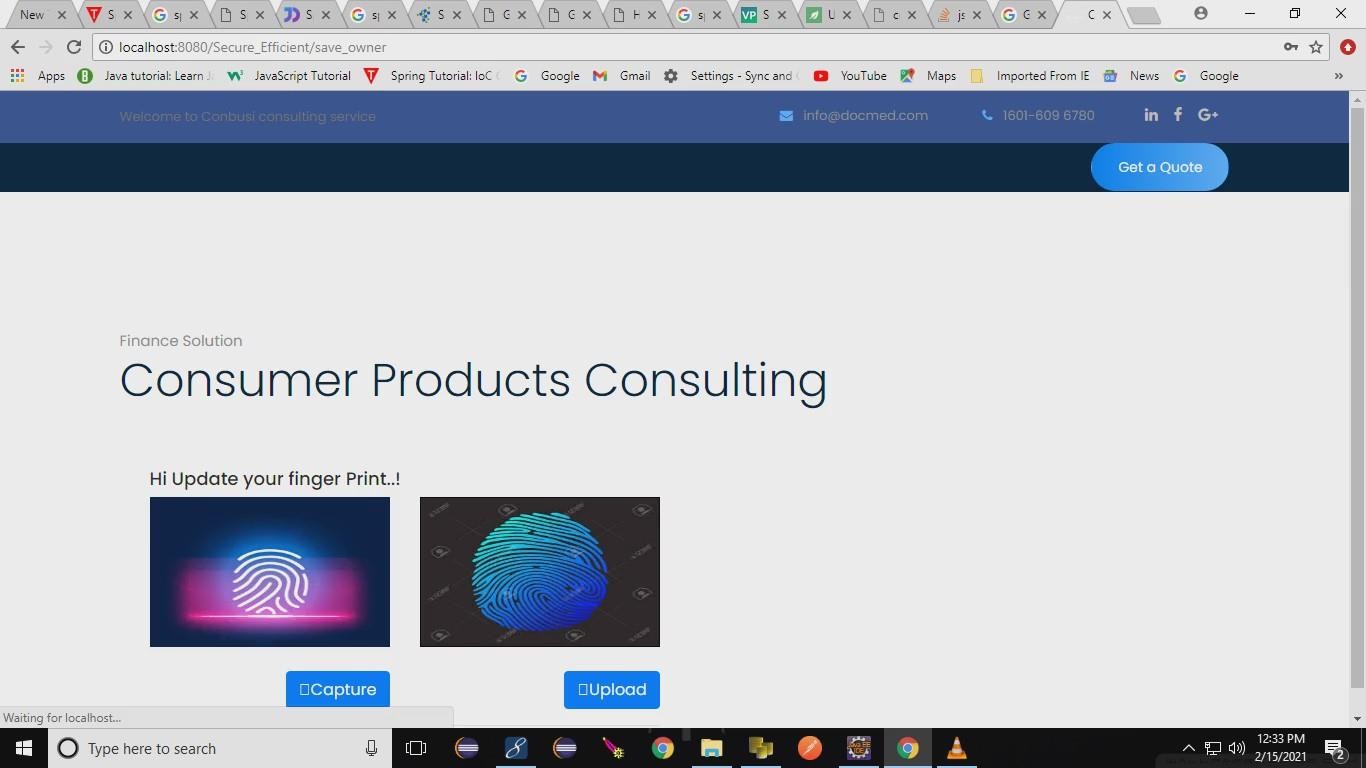
1. Cloud Owner Upload File to Cloud Server

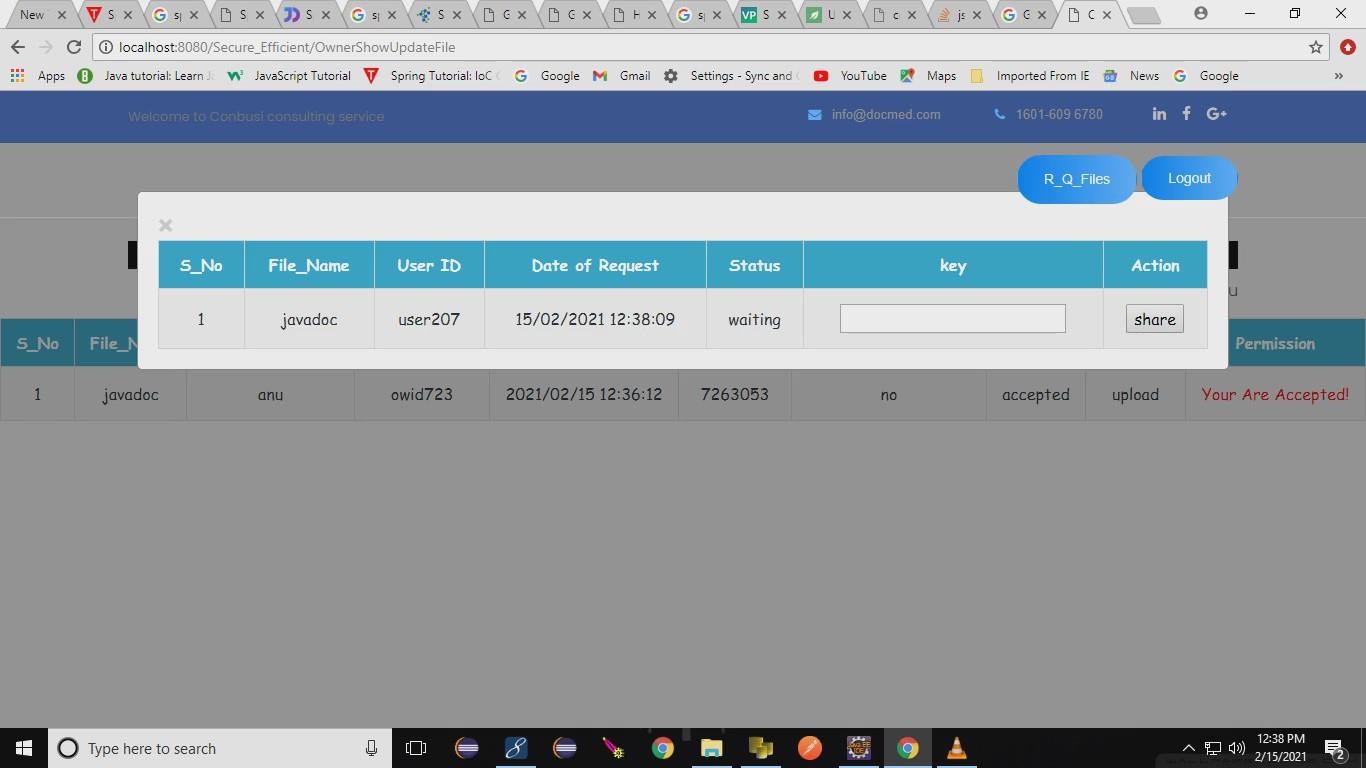
User can able to upload any file in the cloud in order to provide security to the file user need to encrypted the file in the cloud. Cloud contain the only the encrypted format information about the file and corresponding parameter related to the file. In order to maintain security user initially generated the parameter related to the file and along with the mode to upload the data mode as public or private if private then user need to specify the client or mention group of people who can access or download the file then based on this parameter RSA will generate a key and sent to the user based in these key user would encrypt the file and upload to server.

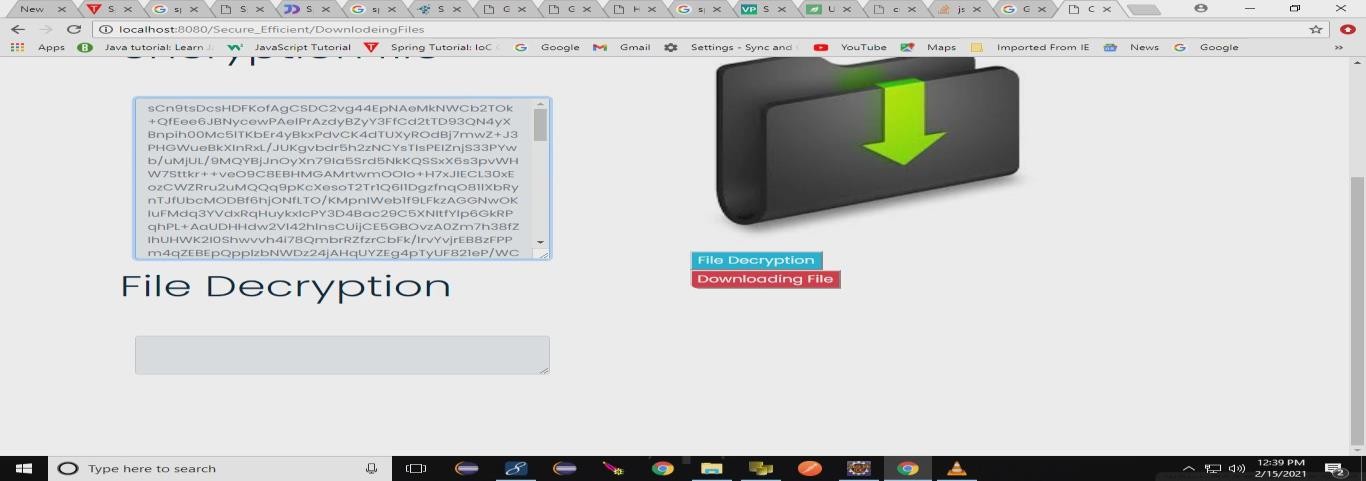
1. Decrypt and Download file:

Then User would search the file based on the parameter if any parameter match in the server, then the server will load the entire related file to that parameter. Before download any file from the sever the user would also need to mutual authentication to the server, if user ﬁngerprint authenticated to the server then he access the file as file is in encrypted format user need to decrypt the file to decrypt the file user request to KGC (Key Generation Centre) for key along with the file parameter and user attribute then user can able to download the file.









# CONCLUSION

In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. 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. The main aim of the project is used to derive a unique identity from the user’s biometric data which is further used to generate the user’s private key.

# REFERENCES

1. C. Yuan, X. Sun, and Q. M. J. Wu, “Difference co-occurrence matrix using BP neural network for fingerprint liveness detection,” Soft Computing, vol. 23, no. 13, pp. 5157–5169, 2019.
2. S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, “Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884– 2895, Aug 2018.
3. Srinivas Jangirala, Mohammad Wazid,”Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things” IEEE Transactions on Dependable and Secure Computing · July 2018
4. Wencheng Yang, Song Wang,Jiankun Hu, Guanglou Zheng and Craig Valli ,”Security and Accuracy of Fingerprint-Based Biometrics: A Review” Received: 2 December 2018; Accepted: 23 January 2019; Published: 28 January 2019
5. Zhihua Xia, Xingming Sun, Neal N. Xiong ,”A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection” IEEE Transactions on Systems, Man, and Cybernetics: Systems · January 2018