e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:05/May-2021 Impact Factor- 5.354 www.irjmets.com

CLOUD BASED BIOMETRIC SECURITY FOR ORGANISATIONS

Abhinaya R*1, Abitha C*2, Priyanka B*3, Salini R*4

*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.

*4Department of CSE Engineering, Panimalar engineering college , Chennai ,Tamil Nadu, India.

ABSTRACT

In this paper, we design a replacement biometric-based authentication protocol to provide secure access to a far off (cloud) server. Additionally, we propose an efficient approach to urge a session key between two communicating parties using two biometric templates for a secure message transmission. An thorough 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. one among the benefits of biometric cryptosystems is that they will bind or directly generate a cryptographic key, which may be used for both authentication and encoding.

Keywords: Authentication, Biometric-based security, Cloud service access, Session key.

I. INTRODUCTION

To generate a revocable private key directly from an irrevocable fingerprint image. there's no got to store the private key or an immediate sort of the user's biometric data anywhere. The scheme is extremely efficient because it uses only cryptographic hash function alongside the symmetric encryption/decryption. A user can access the knowledge of any smart device of monitoring group through the central controller,

II. 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.

Proposed system

In Proposed system, Cloud contains the encrypted information alongside the parameter associated with that file. Supported the attribute cloud will redirect all the related file to the user so as to decrypt the file user need the key for that file for that user request to RSA and DSE (Key Generation Centre) with the fileattributes.

Cloud services are a norm in our society. However, providing secure access to cloud services isn't a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise. variety of authentication mechanisms are proposed within the literature, like those supported Kerberos, OAuth and OpenID. Generally, these protocols seek to determine a secure delegated access mechanism among two communicating entities connected during a distributed system. These protocols are supported the underlying assumption that the remote server liable for authentication may be a trusted entity within the network. Specifically, a user first registers with a foreign server. this is often needed to make sure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and therefore the user also authenticates the server. Once both verifications are successfully administered, 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 within the authentication server, which may be stolen and misused to realize unauthorized access to varied services. Also, to make sure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which needs variety of cryptographic keys to be shared during the authentication process. This strategy leads to an overhead to the authentication protocols.

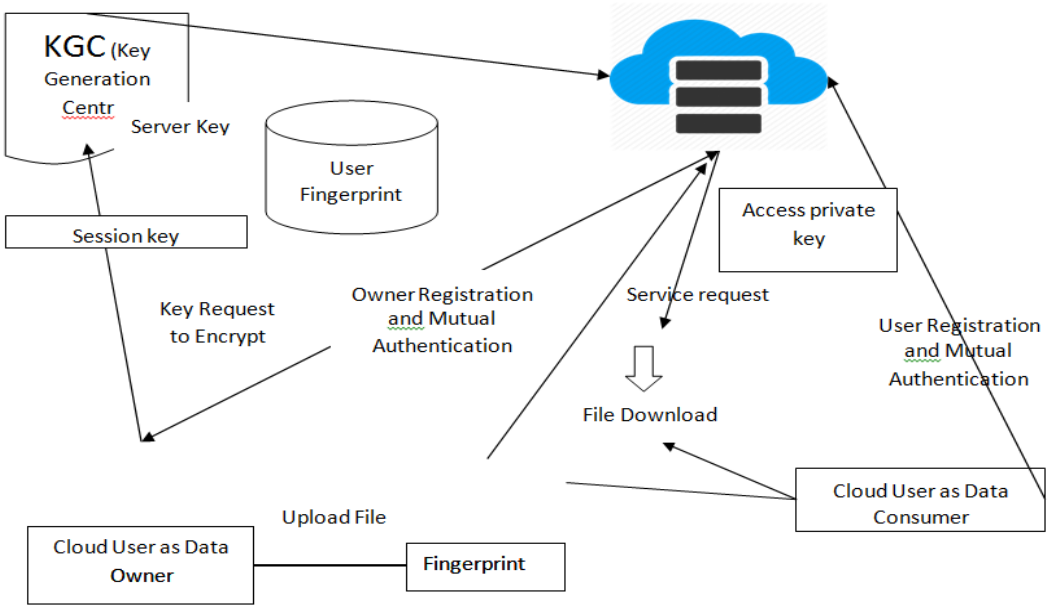
Therefore, during this paper we seek to style a secure and efficient authentication protocol. Specifically, we'll

first provide an alternate to standard password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved within the authentication protocol, without having any secret pre-loaded (i.e., shared) information. within the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, generate a personal key that's want to enroll the user's credential secretly within the database of an authentication server. within the authentication phase, we capture a replacement biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a question. 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 prepared to access his/her service from the specified server. to get secure access to the service server, mutual authentication between the user and authentication server, and also between the user and repair server are proposed employing a short-term session key. Using two fingerprint data, we present a quick and robust approach to get the session key. Additionally, a biometric based message authenticator is additionally generated for message authenticity purpose.

ADVANTAGES

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

BLOCK DIAGRAM DESCRIPTION



III. 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.

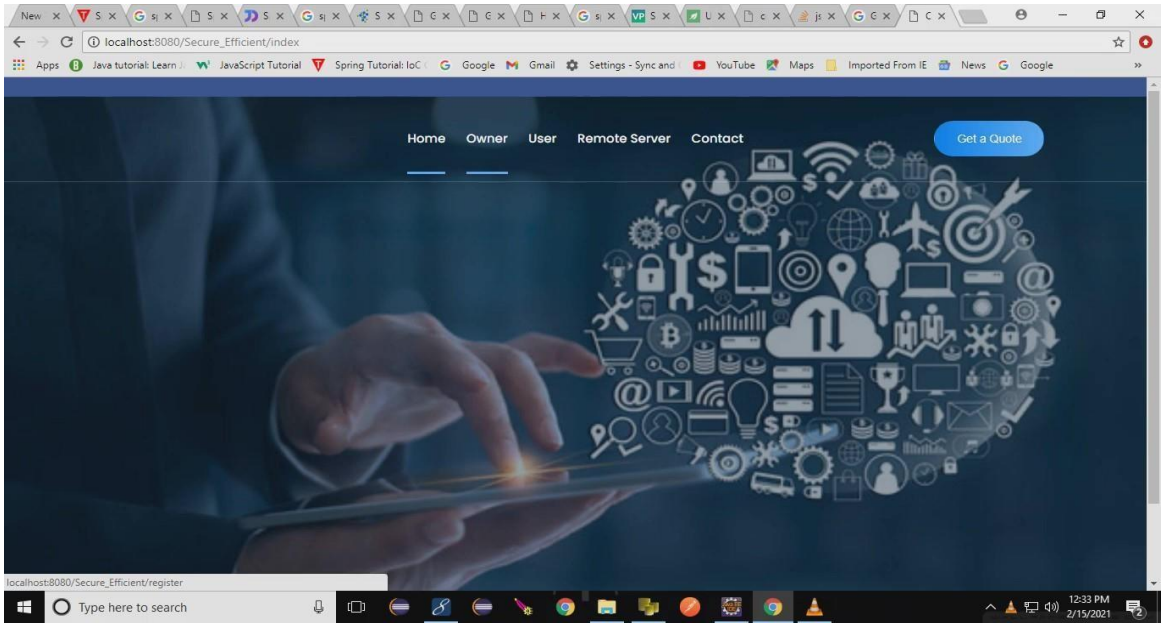
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:05/May-2021 Impact Factor- 5.354 www.irjmets.com

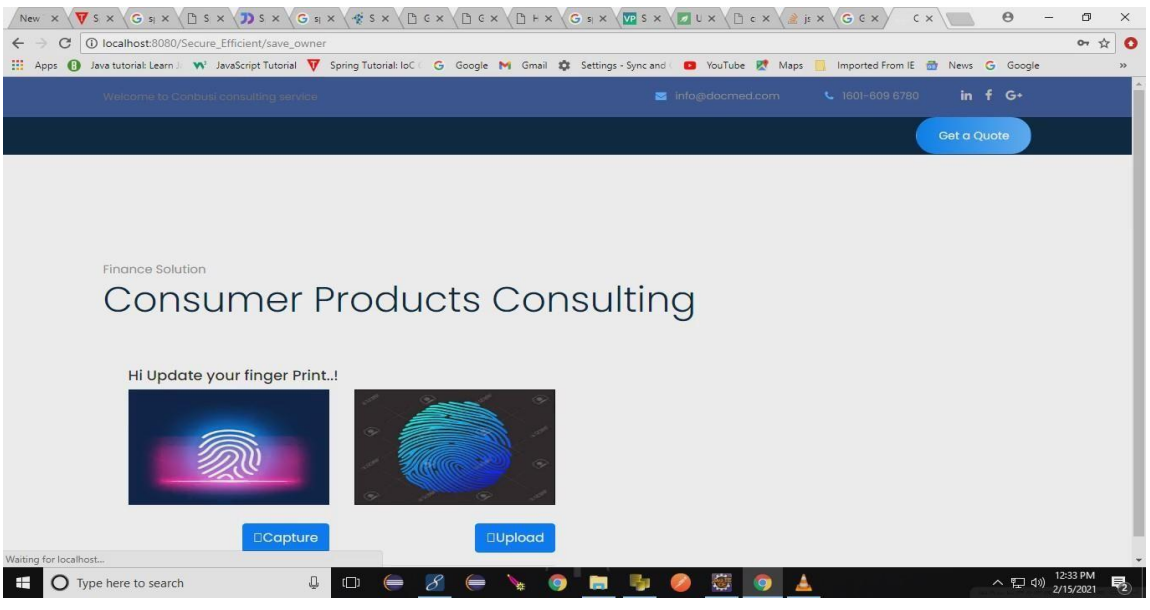
2.Cloud Owner Upload File to Cloud Server

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.

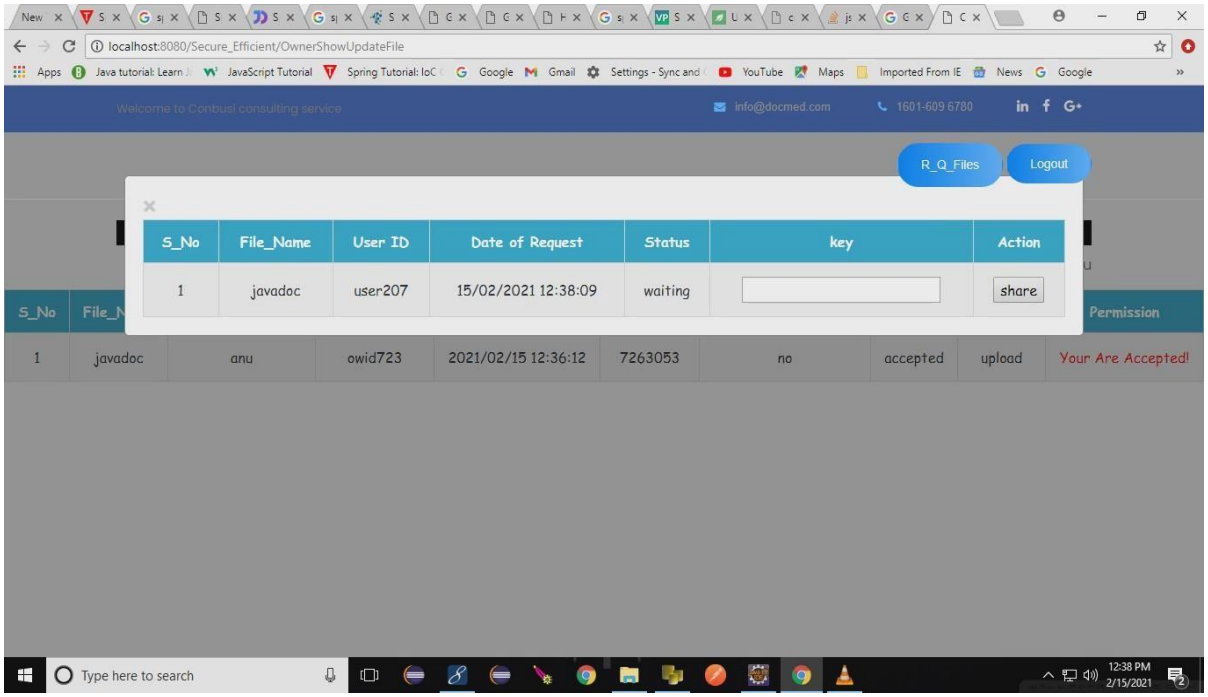
3. Decrypt and Download file:

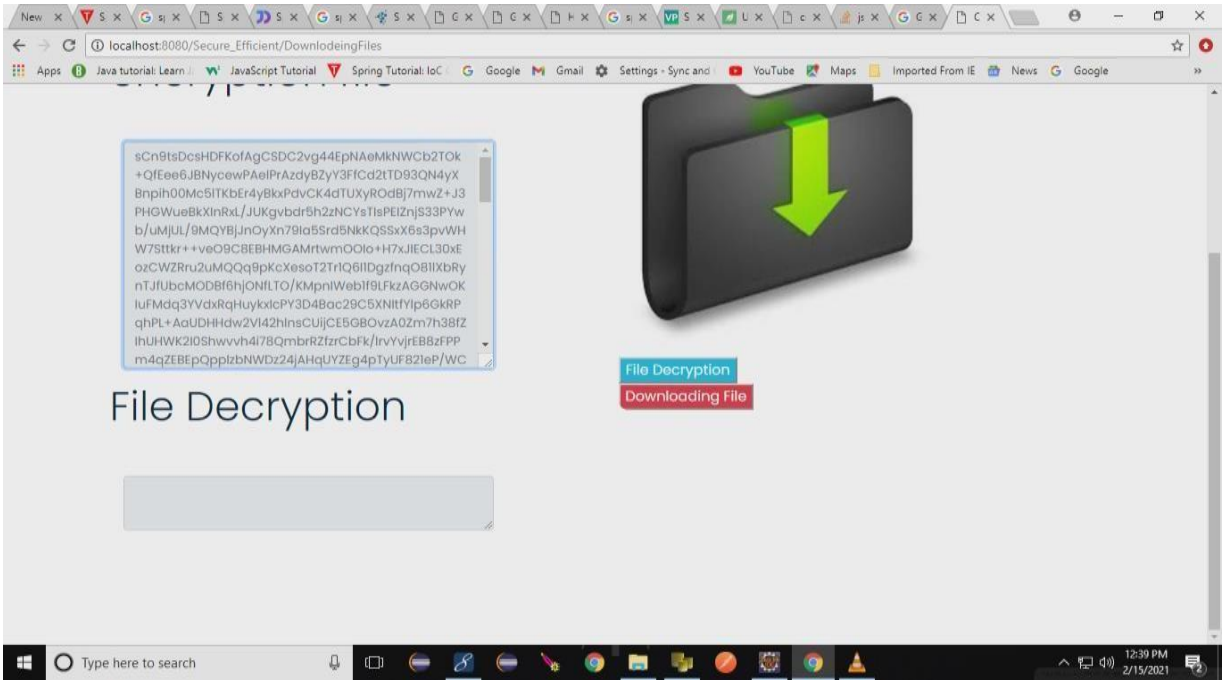
Then User would search the file based on the parameter if any parameter match in the server, then the server will load the entire related file to that parameter. Before download any file from the sever the user would also need to mutual authentication to the server, if user fingerprint authenticated 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.





e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:05/May-2021 Impact Factor- 5.354 www.irjmets.com





IV. CONCLUSION

In this paper, we design a replacement biometric-based authentication protocol to provide secure access to a far off (cloud) server. Additionally, we propose an efficient approach to urge 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 thus the session key's generated without sharing any prior information. the most aim of the project is employed to derive a singular identity from the user's biometric data which is further wont to generate the user's private key.

V. 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