JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

Designing Secure And Efficient Biometric-Based Secure Access Mechanism For Cloud Services

Dr.Baby Munirathinam[1], B.Amulya[2], D.Chandana [3], G.soumya[4], G.Sushma[5]

[2,3,4,5] UG Scholars, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.

[1]Assistant Professor, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, 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.

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

1.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. 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.

2.LITERATURE SURVEY

2.1 Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment

AUTHORS: A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues,

ABSTRACT:

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.

2.2 Security and Accuracy of Fingerprint-Based Biometrics: A Review

AUTHORS: W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli

ABSTRACT: 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.

2.3 Difference co-occurrence matrix using BP neural network for fingerprint liveness detection

AUTHORS: C. Yuan, X. Sun, and Q. M. J. Wu

ABSTRACT: With the growing use of fingerprint identification systems in recent years, preventing fingerprint identification systems from being spoofed by artificial fake fingerprints has become a critical problem. In this paper, we put forward a novel method to detect fingerprint liveness based on BP neural network, which is used for the first time in the fingerprint liveness detection. Moreover, different from traditional detection methods, we propose a scheme to construct the input data and corresponding category labels. More effective and efficient texture features of fingerprints, which are used as the input data of the BP neural network, are computed to improve classification performance and obtain a better pre-trained network model. After a variety of preprocessing operations and image compression operations, gradient values in the horizontal and vertical directions are computed by using Laplacian operator, and difference co-occurrence matrices are constructed from the obtained gradient values. Then, the input data of neural network model are built based on two DCMs. The pre-trained neural network models with diverse neuron nodes are learnt. Different experiments based on different parameters for the BP neural network have been conducted. Finally, classification accuracy of testing fingerprints is predicted based on the pre-trained networks. Experimental results on the LivDet 2013 show that the classification performance of our proposed method is effective and meanwhile provides a better detection accuracy compared with the majority of previously published results.

2.4 An Untraceable Biometric-Based Multi-server Authenticated Key Agreement Protocol with Revocation

AUTHORS: C.-C. Chang and N.-T. Nguyen,

ABSTRACT: Online access has been widely adopted to distribute diversified services to customers. In this architecture, public channels are utilized to exchange information between end users and remote servers at anytime and anywhere. To achieve confidentiality and integrity for transferred data, the related parties have to authenticate each other and negotiate a secret session key to encrypt and decrypt exchanged messages. Since the Lamport's pioneering authentication work in 1981, numerous mechanisms have been proposed to enhance security as well as reduce computation and payload data. Recently, Chuang and Chen proposed a multi-server authenticated agreement protocol employing a smart card and biometric data to eliminate the weaknesses caused by parameters related to low-entropy human-memorable passwords that are stored in a physical location. However, Mishra et al. showed that Chuang and Chen's protocol is not only vulnerable to multiple attacks but also suffers from the drawback of variation of biometric data. To overcome these weaknesses, they proposed an enhanced three-factor authenticated key agreement protocol using the low-error rate Biohashing technique.

Unfortunately, we found that Mishra et al.'s scheme is also vulnerable to the denial-of-service attack, the traceable user attack, the impersonation attack, and the pre-shared key attack. Furthermore, the protocol does not provide any user revocation mechanism to control user accesses. In this novel untraceable authenticated key agreement scheme, we adopt the Hamming distance to verify encrypted Biohash codes and a public-key technique to construct the revocation mechanism. Our scheme achieves not only zero errors of biometric verification but also secure against all known attacks.

2.5 A secure temporal-credentialbased mutual authentication and key agreement scheme for wireless sensor networks

AUTHORS: D. He, N. Kumar, and N. Chilamkurti,

ABSTRACT: With the development of wireless communication technology and sensor technology, the wireless sensor network (WSN) has been widely used in various applications, such as military surveillance, environment monitoring industry control, medical monitoring, and so on. In most of the cases, WSNs are deployed in unattended environment. So, these are more vulnerable to various attacks than traditional networks. To protect communications in WSNs, mutual authentication and key agreement schemes for WSNs have been studied widely. Recently, Xue et al. proposed a temporal-credential-based mutual authentication and key agreement scheme for WSNs and claimed their scheme could withstand various attacks. However, in this paper, we will point out that their scheme is vulnerable to the off-line password guessing attack, the user impersonation attack, the sensor node impersonation attack and the modification attack. To overcome weaknesses in Xue et al.'s scheme, we also propose a new temporal-credential-based mutual authentication and key agreement scheme for WSNs. Security analysis shows our scheme could overcome weaknesses in Xue et al.'s scheme. Performance analysis shows our scheme also has better performance. Therefore, our scheme is more suitable for providing secure communication in WSNs.

3.SYSTEM ANALYSIS

3.1EXISTING 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.

3.2 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

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

authentication protocols (i.e., Message Authentication Code (MAC)), is introduced.

Advantages:

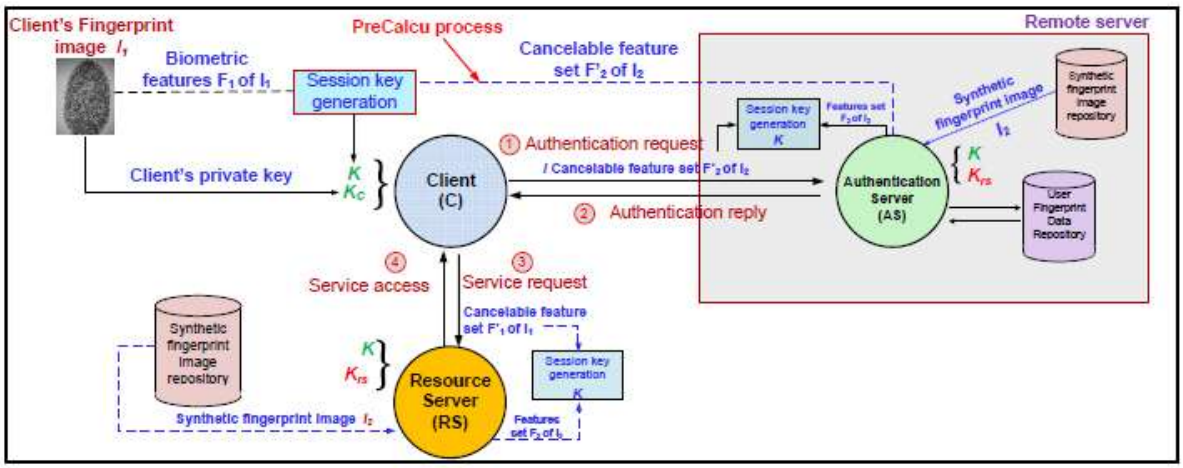
1. An efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission.

2.There is no need to store the user's private key anywhere and the session key is generated without sharing any prior information.

3.3 SYSTEM REQUIREMENTS:

This section elaborates on the functional requirements of the application. The SRS itself can be divided into module, each module having specifications. In order to carry out the project, the following hardware and software is required.

SYSTEM ARCHITECTURE:



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

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

add synthetic fingerprint images.Admin can able to view the data in the repository.

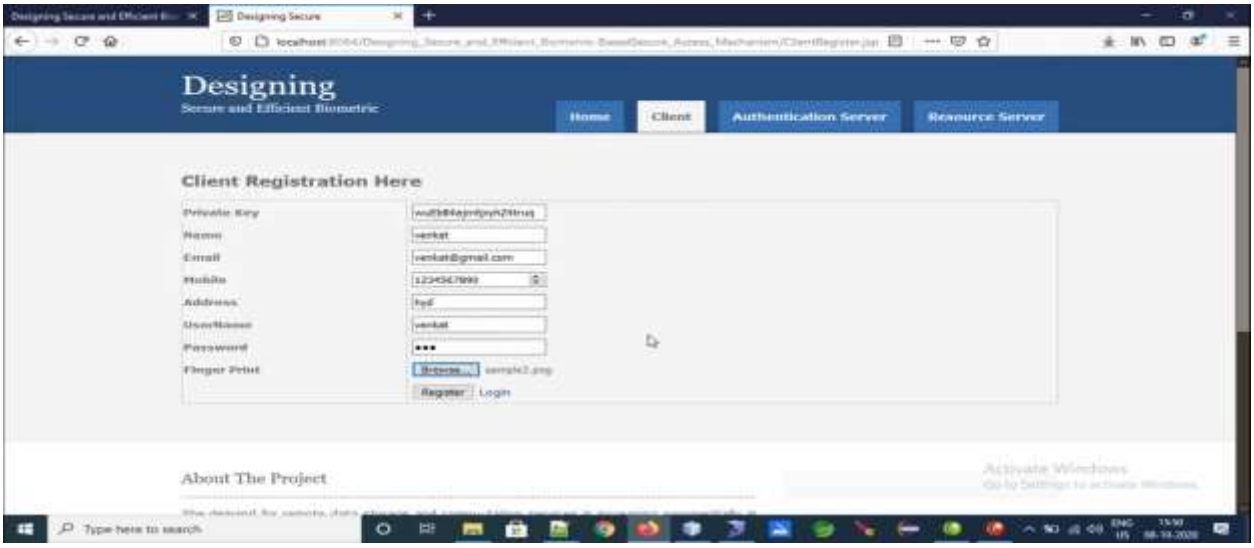
4.RESOURCE SERVER

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

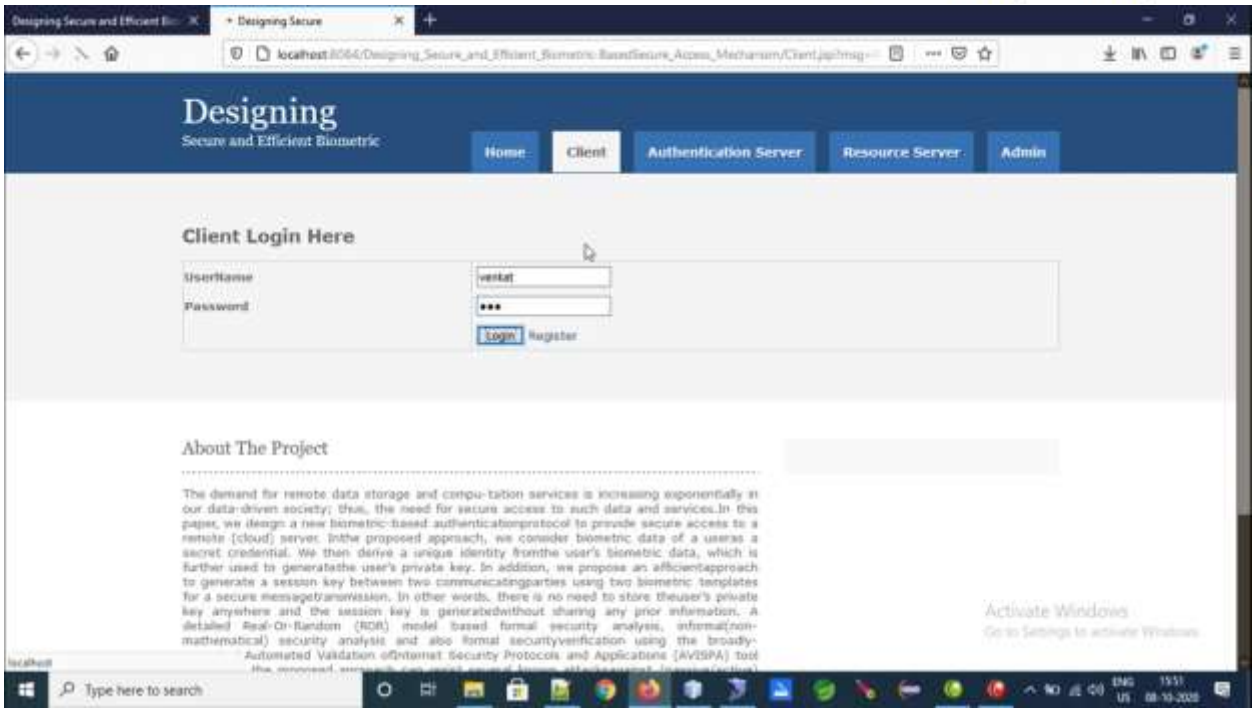
Home Page

Client Registration

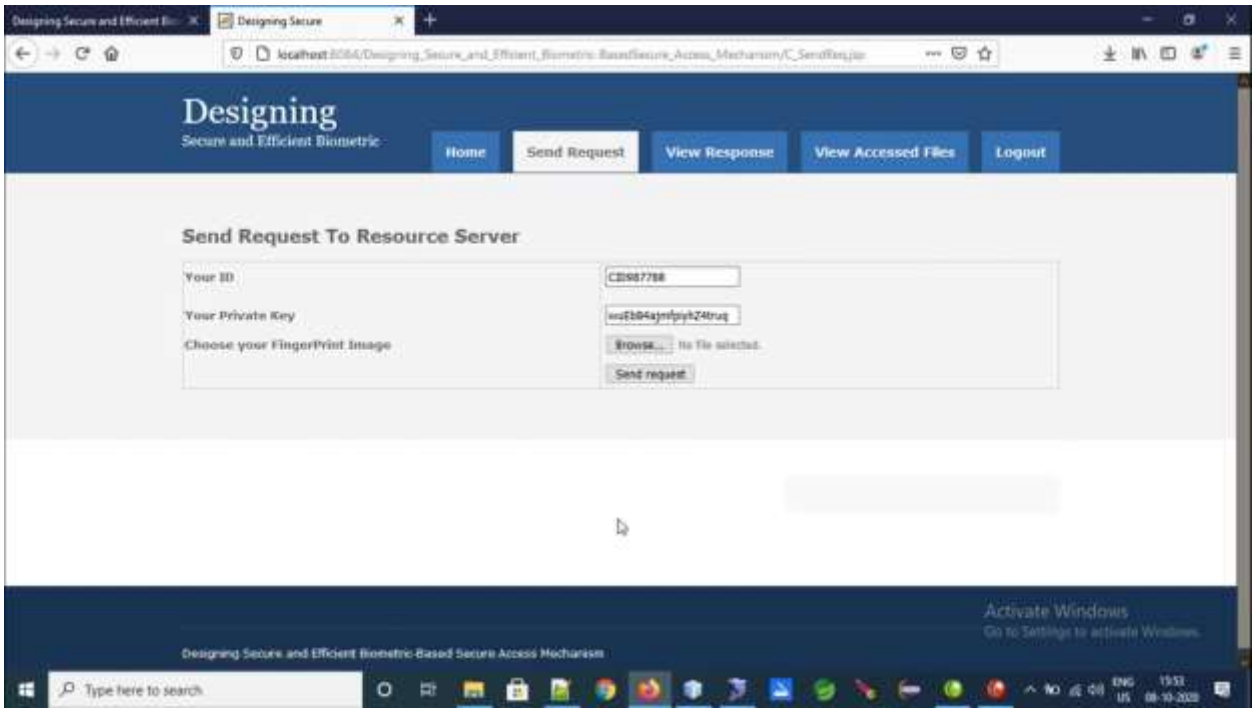


Client Login

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

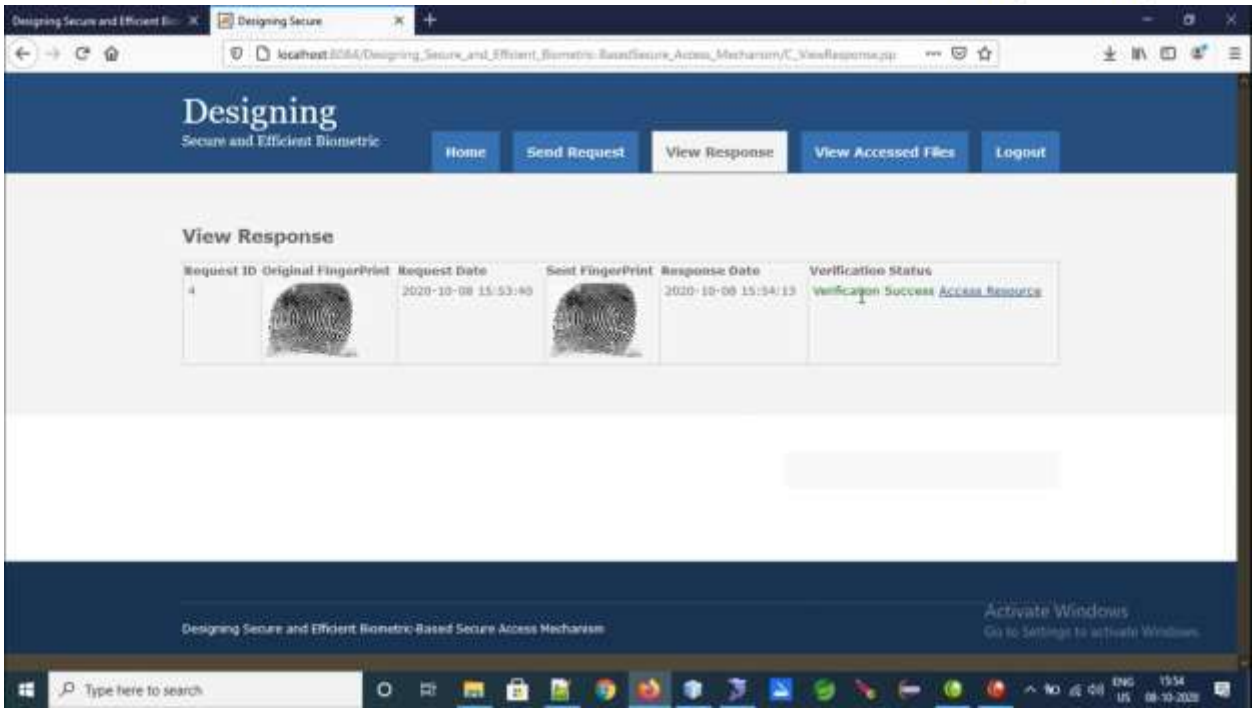


Send Request

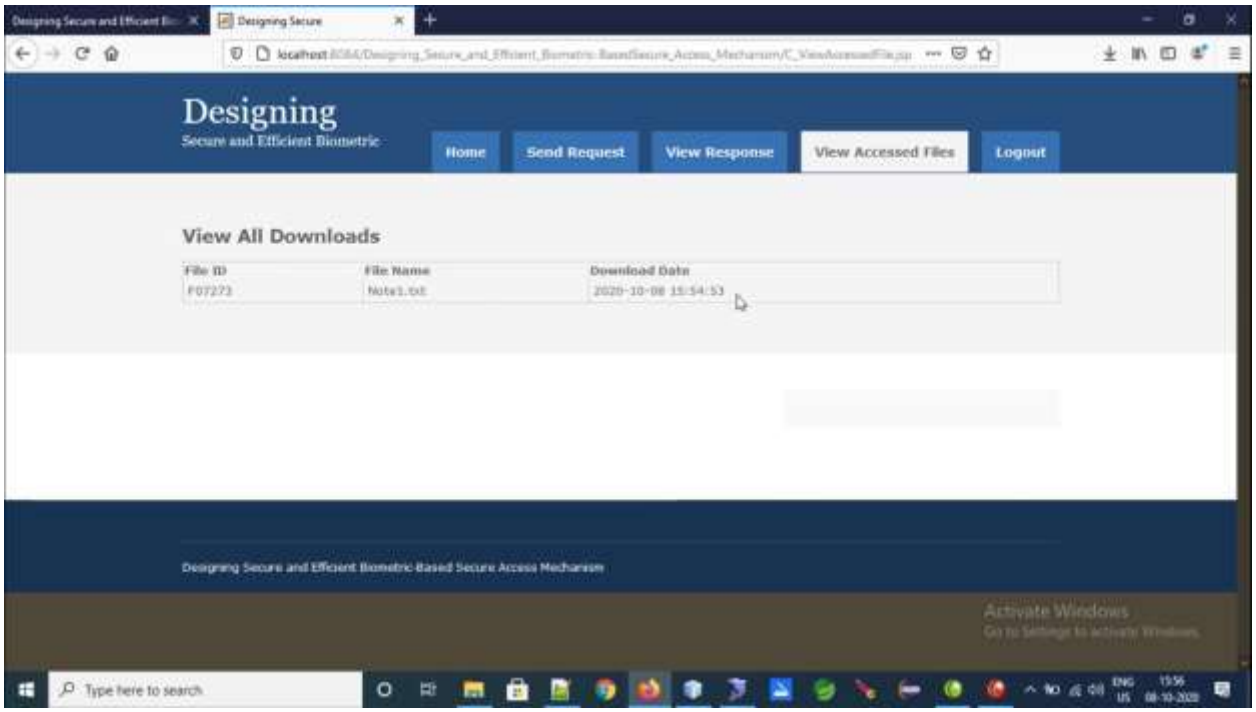


View Response

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

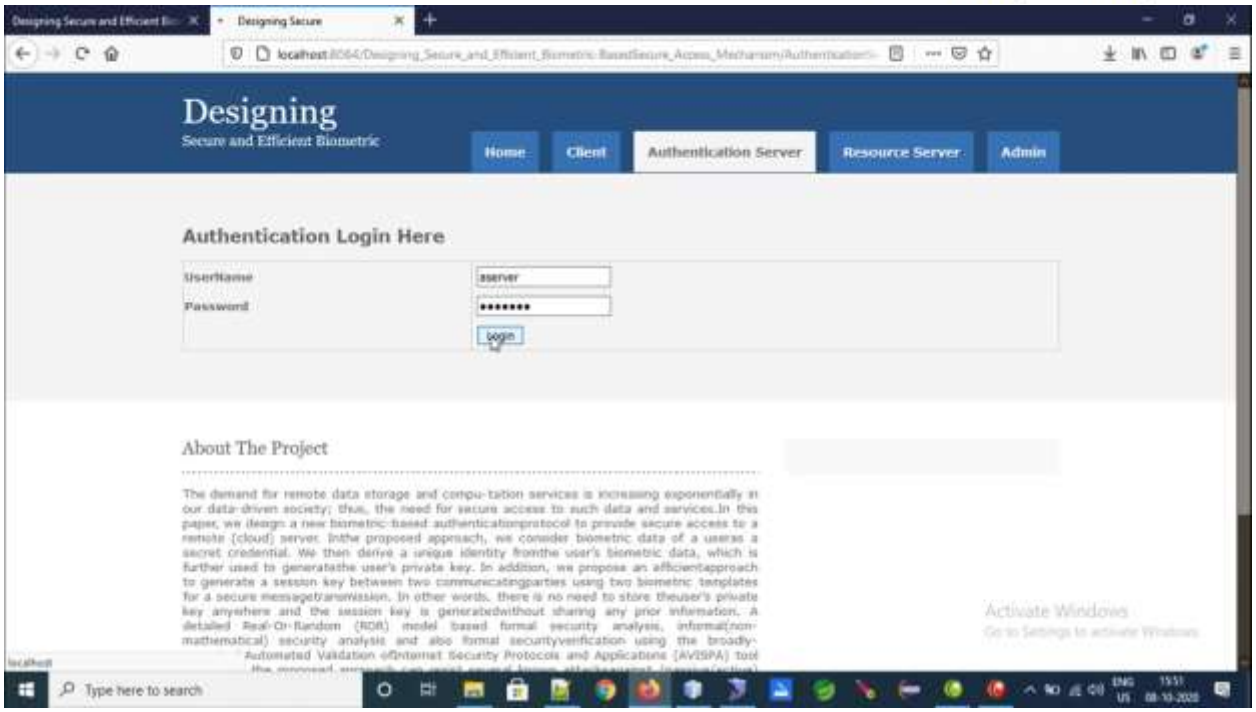


View Accessed Files

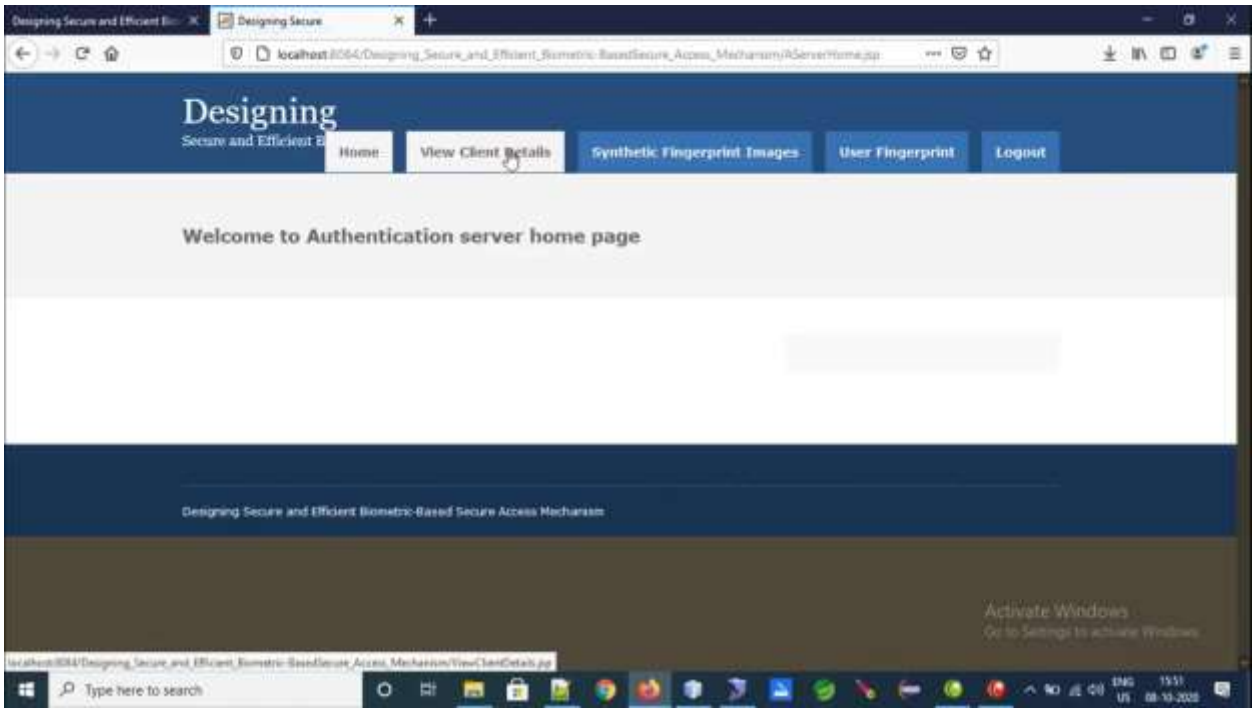


Authentication Server

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

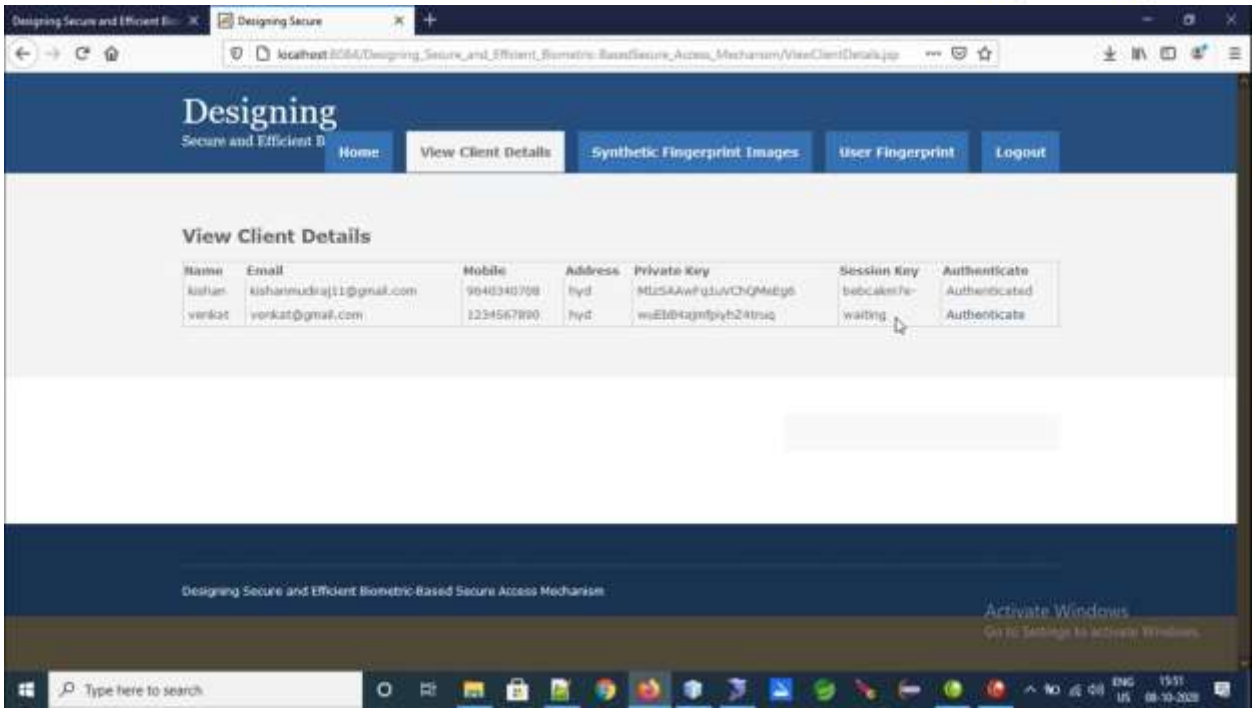


Authentication server Home

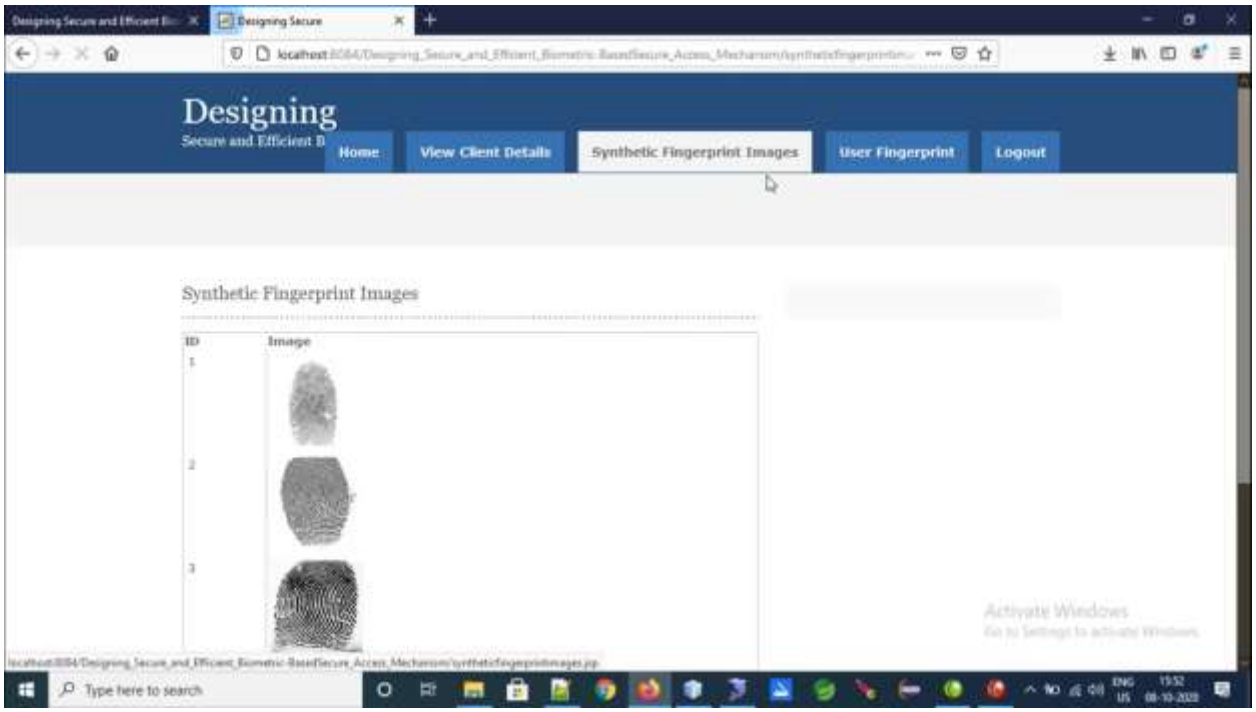


View Client Details

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

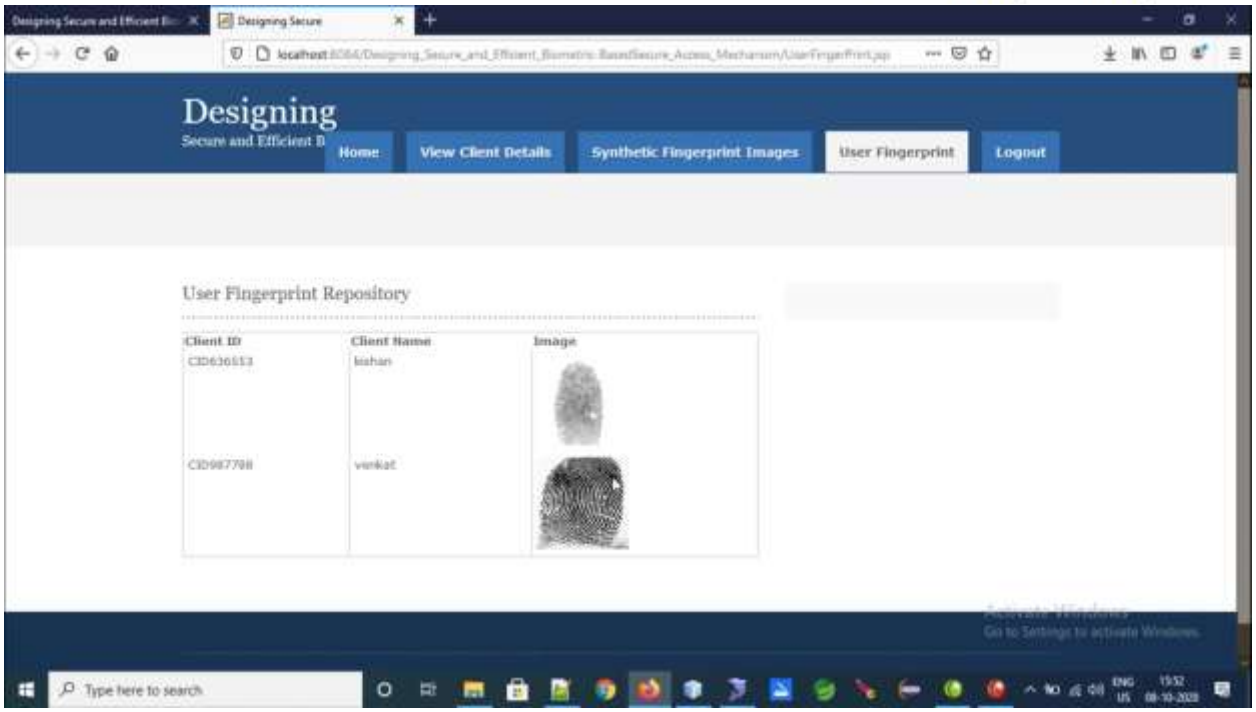


Synthetic Fingerprint Images

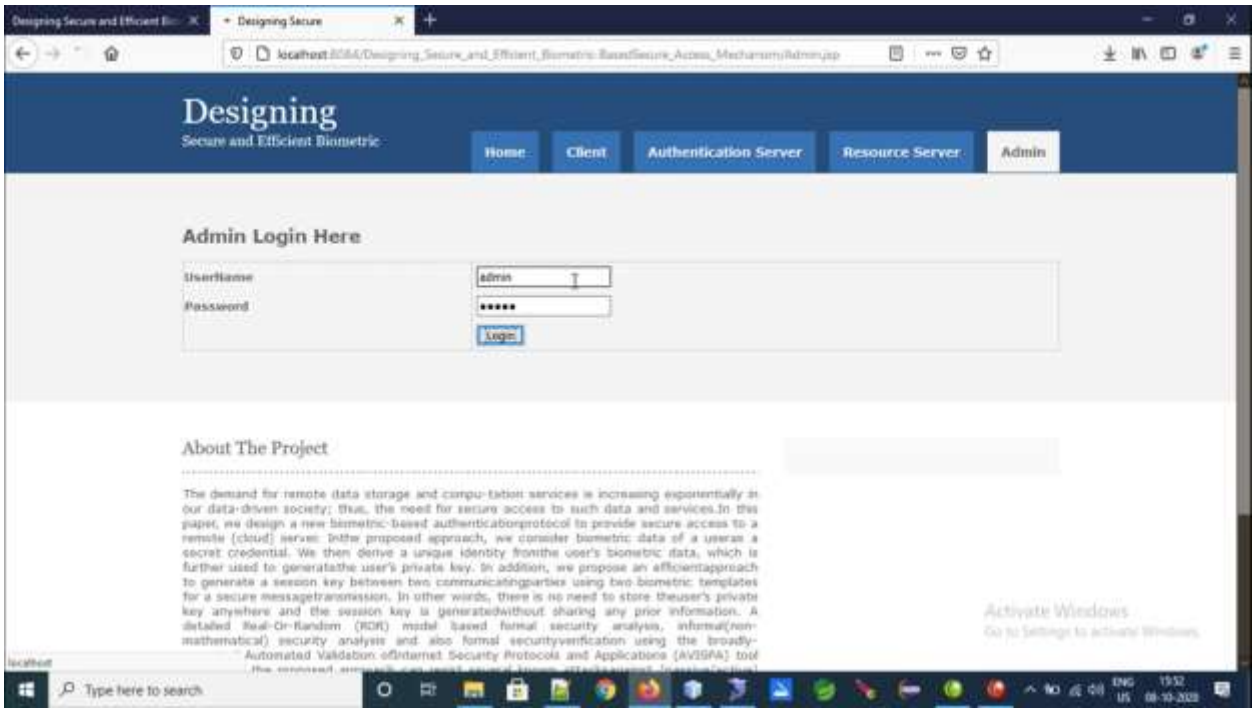


User Fingerprint

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

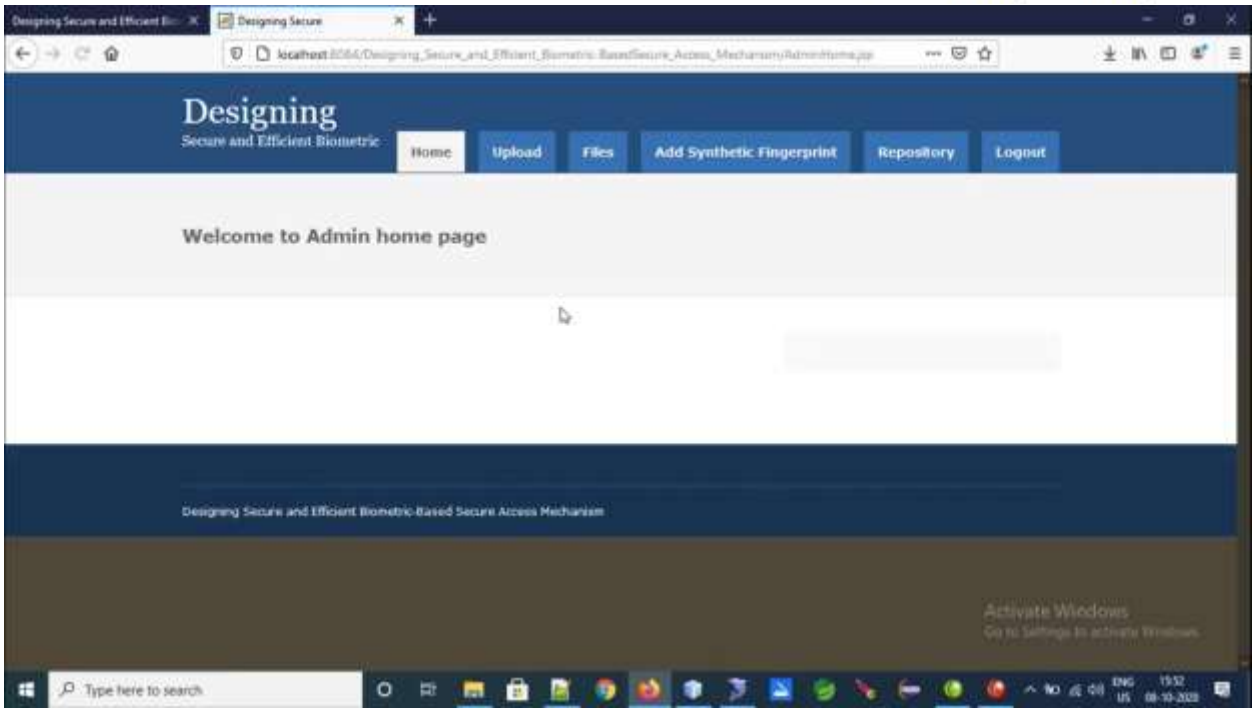


Admin

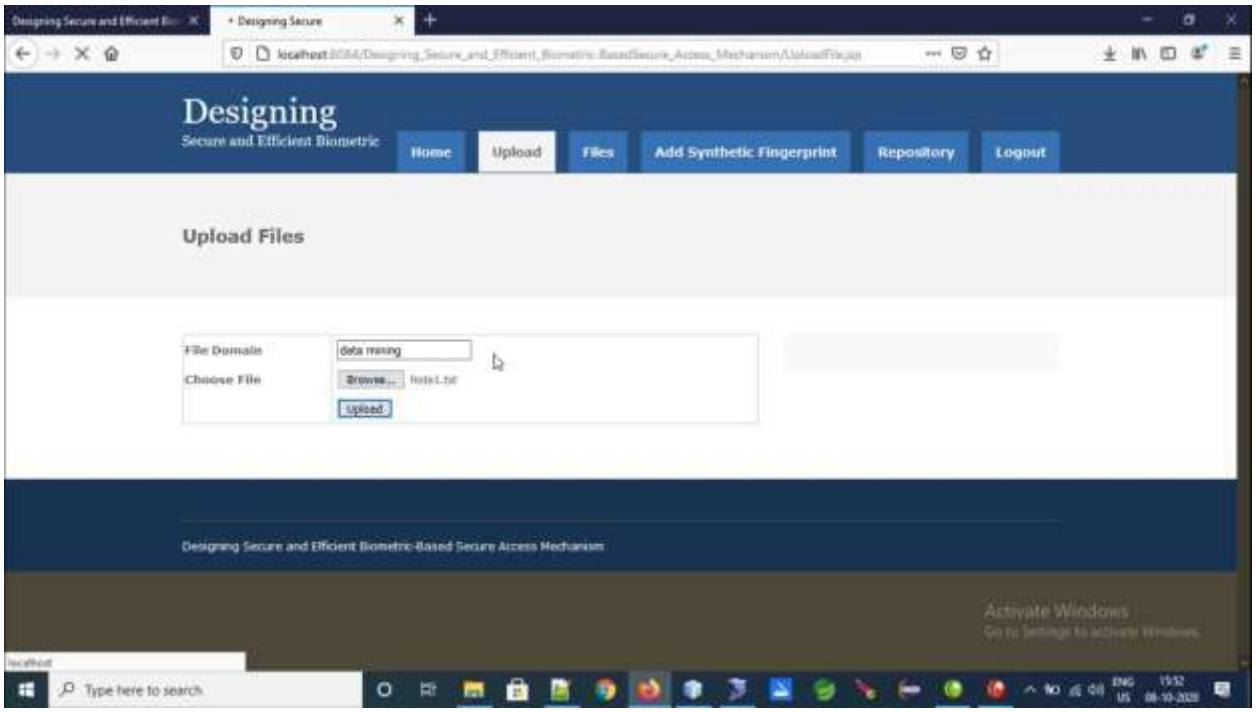


Admin Home Page

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

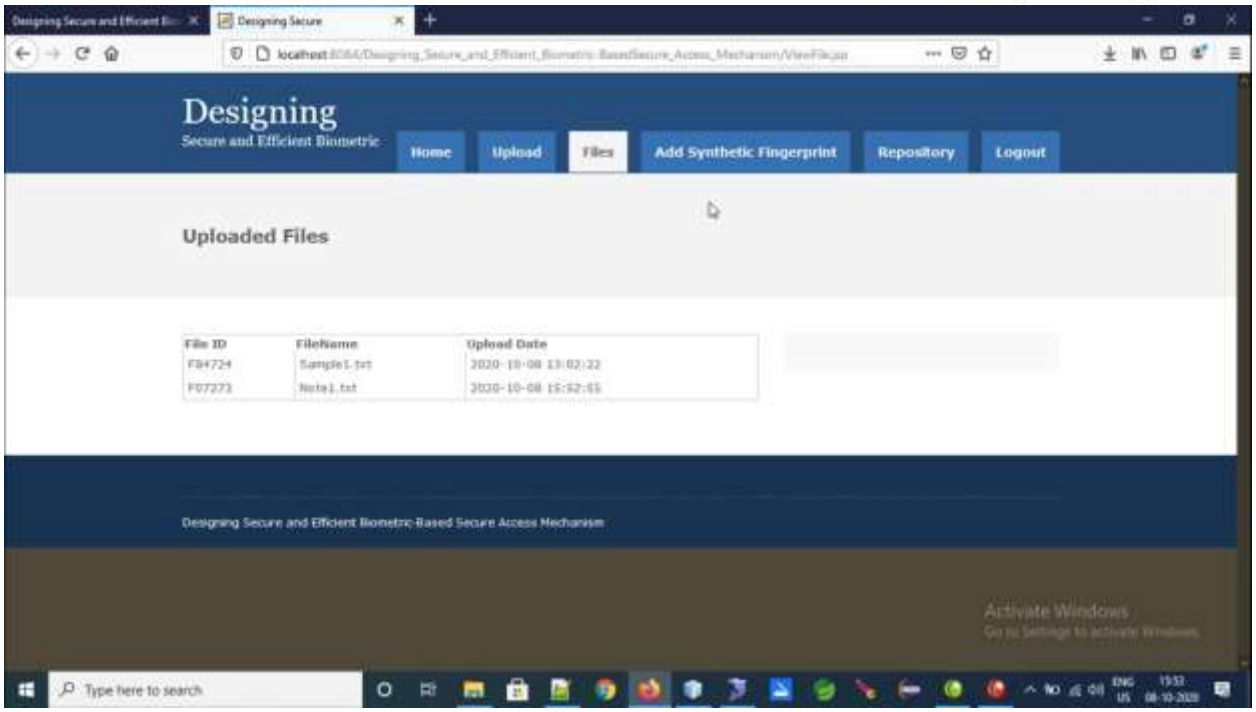


Upload Files

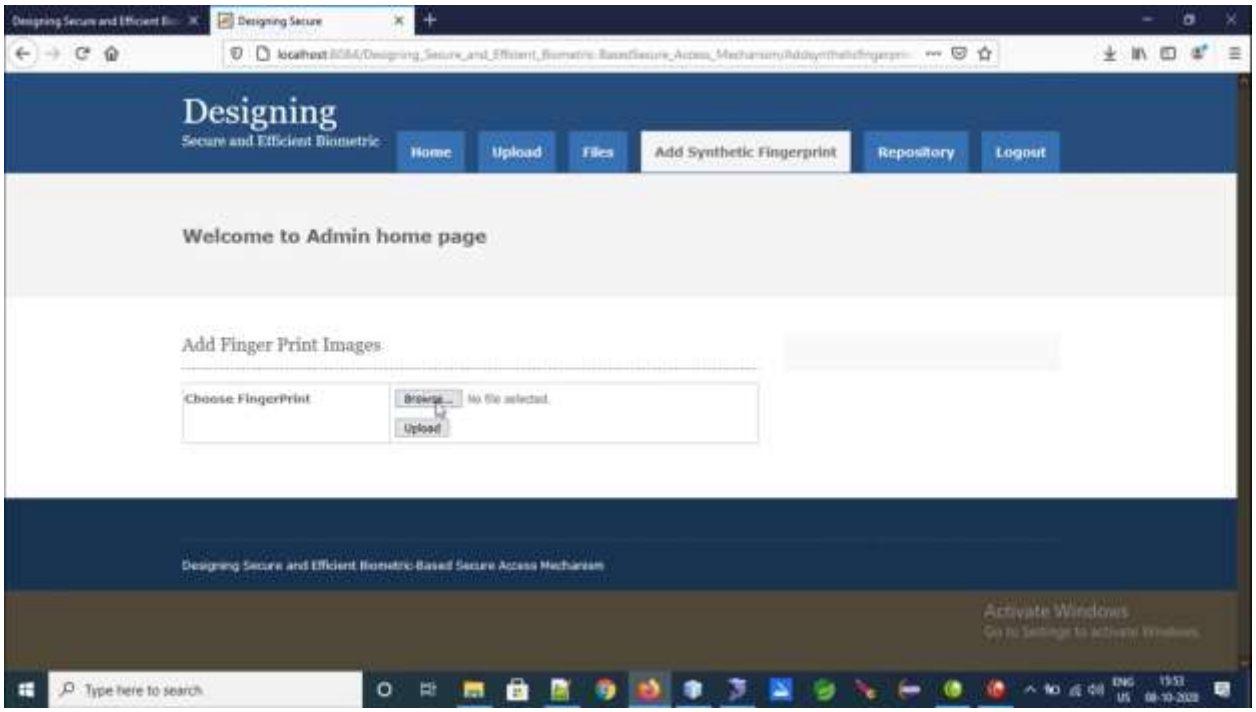


Files

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

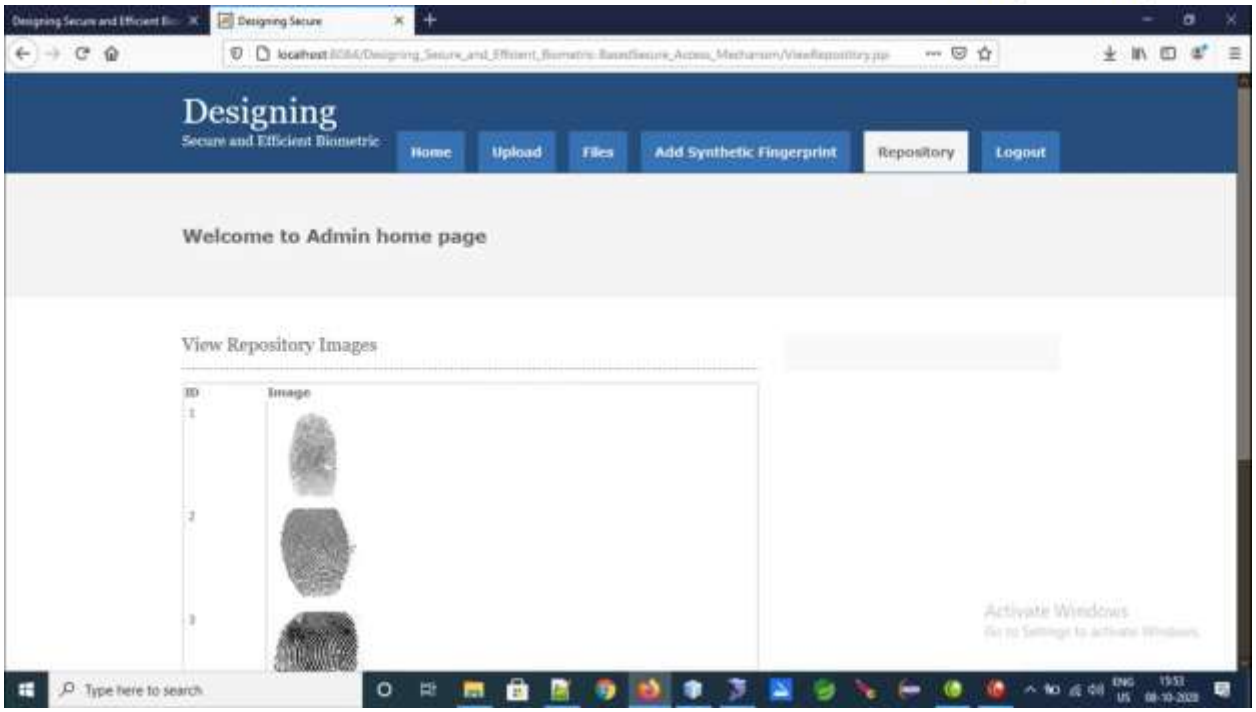


Add Synthetic Fingerprint

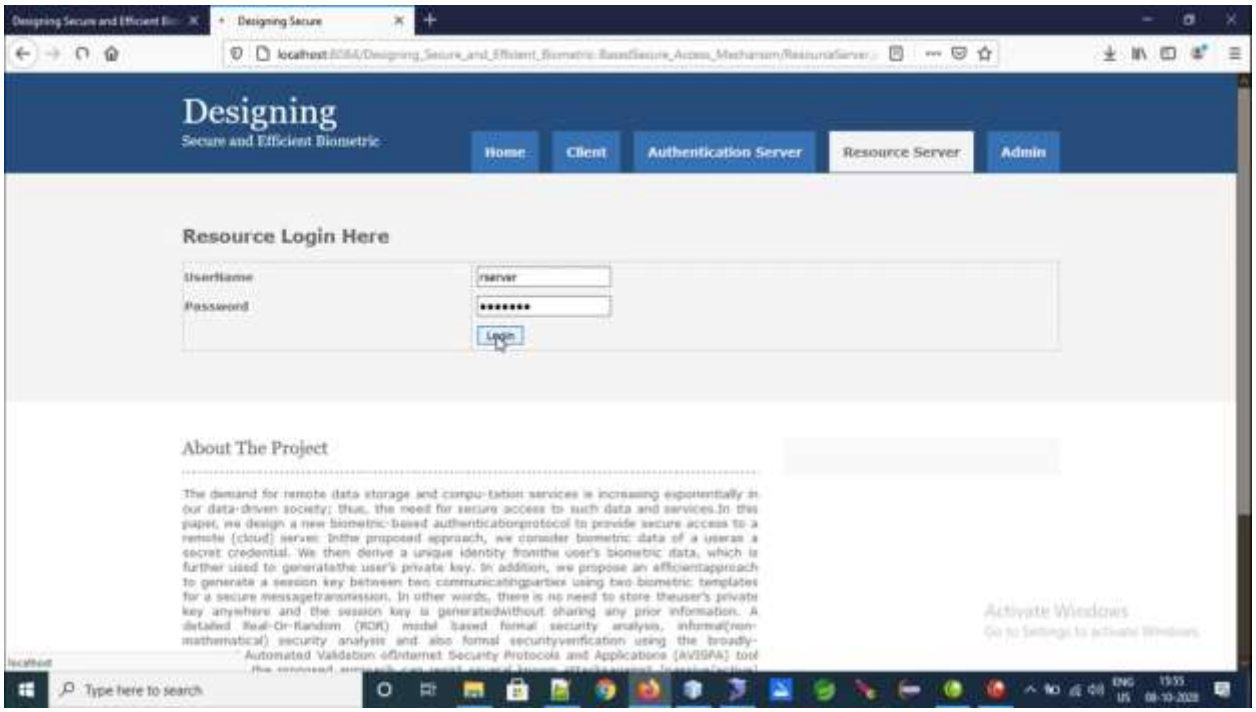


Repositorty

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023

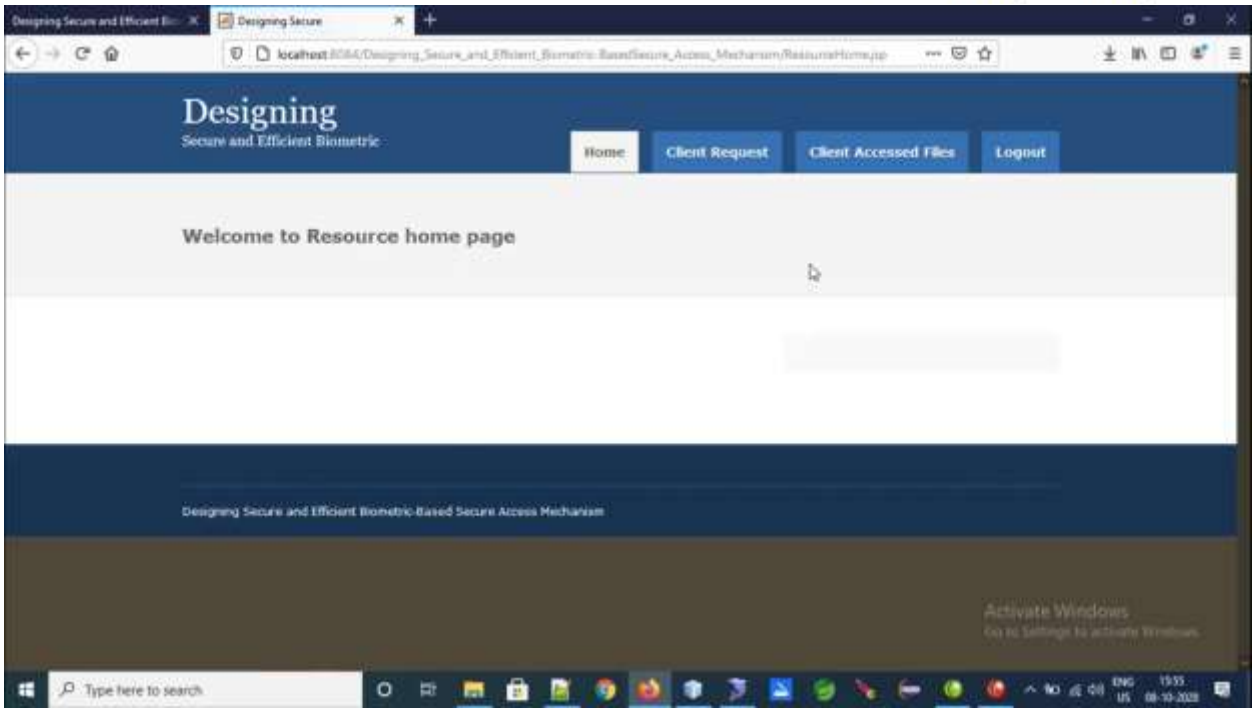


Resource Server

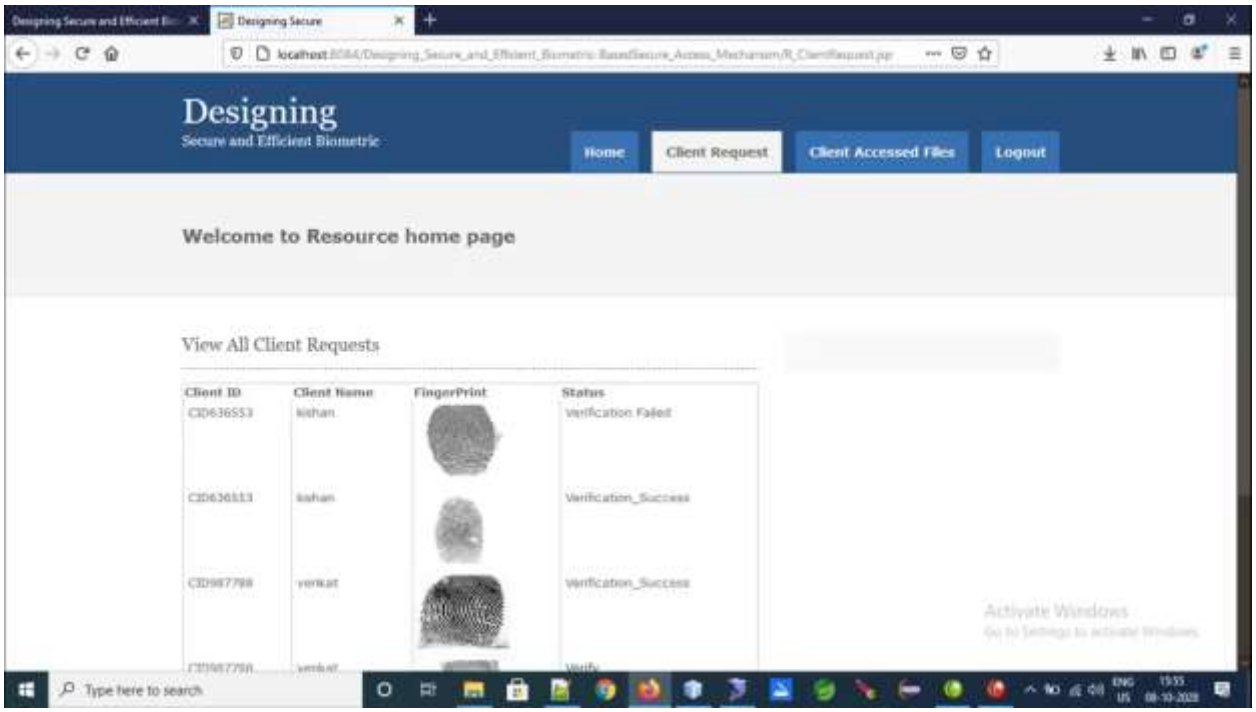


Rserver homepage

ISSN- 2394-5125 VOL 10, ISSUE 07, 2023



Client Request



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, 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 Infomration 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.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," ACM Wireless Networking, 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," Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.

[11] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[12] M. Walla, "Kerberos explained," Windows 2000 Advantage Magazine, 2000.

[13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015. [14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An efficient biometric authentication protocol for wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013, Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971. [15] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," Journal of

Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.

[16] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," Ad Hoc Networks, vol. 20, pp. 96 – 112, 2014. [17] M. Park, H. Kim, and S. Lee, "Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards," in 17th International Conference on Computational Science and Engineering, Chengdu, China, 2014, pp. 1541–1544. [18] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255 – 270, 2017.

[19] S. D. Kaul and A. K. Awasthi, "Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement," Wireless Personal Communications, vol. 89, no. 2, pp. 621–637, 2016.

[20] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient and Secure Biometric-Based User Authenticated Key Agreement Scheme with Anonymity," Security and Communication Networks, vol. 2018, pp. 1–14, 2018, Article ID 9046064, https://doi.org/10.1155/2018/9046064.

[21] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[22] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 9, no. 1, pp. 223–244, 2016.

[23] "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," International Journal of Communication Systems, vol. 30, no. 1, pp. 1–25, 2017.

[24] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credentialbased security scheme with mutual authentication and key agreement for wireless sensor networks," Sensors, vol. 13, no. 8, pp. 9589–9603, 2013.

[25] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credentialbased mutual authentication and key agreement scheme for wireless sensor networks," in International Symposium on Wireless and pervasive Computing (ISWPC), Taipei, Taiwan, 2013, pp. 1–6.

[26] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," ELEKTRONIKA IR ELEKTROTECHNIKA, vol. 19, no. 6, pp. 109 – 116, 2013. [27] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, vol. 36, pp. 58–80, 2016.

[28] C.-C. Chang and N.-T. Nguyen, "An Untraceable Biometric-Based Multi-server Authenticated Key Agreement Protocol with Revocation," Wireless Personal Communications, vol. 90, no. 4, pp. 1695–1715, 2016.

[29] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y. Shi, "A Novel Weber Local Binary Descriptor for Fingerprint Liveness

Detection," IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, doi: 10.1109/TSMC.2018.2874281.

[30] 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.

[31] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," Symmetry, vol. 11, no. 2, 2019. [Online]. Available: https://www.mdpi.com/2073-8994/11/2/141

[32] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1767–1775, 2014.