Efficient Biometric Service Protocol for Cloud Services

SwathiGowroju*, S. Sai Satyanarayana Reddy[2], V. Swathi[3], R. Srinija[4],
P. Rishika[5], K Naveen Reddy[6]

1Associate Professor, Sreyas Institute of Engineering and Technology
2Professor, Sreyas Institute of Engineering and Technology
3,4,5,6 Sreyas Institute of Engineering and Technology

Email: swathigowroju@sreyas.ac.in

ABSTRACT

Cloud services will be ones that can be accessed from a scattered cloud stockpiling worker rather than an on-site server. These measured systems are operated by an outsider and allow users online access to PC resources like systems administration or research. Cloud computing is used to store data on cloud workers and to distribute processing resources across the Internet. Due to the pooling of resources, security and data insurance have become a crucial area of concern in cloud computing. Cloud service providers use server farms that are affected by information spillage to store and keep customer data. It has been noted that several techniques have prioritised data protection while ignoring privacy in the execution. Authentication helps to safeguard and confirm a recipient's identity. We also offer a practical method for creating a session key between two interacting parties that makes use of two biometric models for secure message delivery. Finally, thorough tests and a comparison analysis were used to determine the validity and usefulness of the suggested remedy. Index Terms: Session key, cloud service access, biometric-based security, and authentication.

Keywords: *Bio-Metrics, Fingerprint, Authentication, Cloud*

1. INTRODUCTION

In current world, cloud services are typical. However, providing safe access to cloud services is not a simple effort, and establishing reliable authentication, authorization, and access accounting is a never-ending problem, both operationally and from a research standpoint. In the literature, a variety of authentication methods have been put forth, including ones based on Kerberos, OAuth, and OpenID technologies. These protocols often aim to create a secure delegated access mechanism between two communicative entities linked in a distributed system. These guidelines are predicated on the fundamental premise that the distant server a trustworthy network entity is in charge of authentication. In particular, a user must first register with a distant server. This is required to guarantee the owner's consent. When a user attempts to visit a server, the distant server verifies their identity. The server is also authenticated by the user and the user. Once if both checks are completed successfully, the user receives using a remote server to access the services.

The fact that the user's credentials are kept on the authentication server, where they can be stolen and (mis)used to obtain unauthorised access to numerous services, is a major drawback of the current authentication techniques. Additionally, present techniques often employ symmetric key cryptography, which necessitates the sharing of a number of cryptographic keys throughout the authentication process, to ensure safe and quick communication. The authentication protocols are burdened by this tactic. The flaws found in the published protocols [1-11] are evidence that designing secure and effective authentication protocols is difficult.

We thus aim to provide a reliable and effective authentication technique in this work. We'll start out by offering an alternative to the typical password-based authentication method.

ISBN - 978-93-95038-50-8 https://doi.org/10.37285/bsp.sasat2023.33

Corresponding author: Email: swathigowroju@sreyas.ac.in

Then, without using any shared or pre-loaded information, we show how to create secure communication between the parties participating in the authentication protocol.

According to the suggested method, a user's fingerprint image serves as a secret credential. We create a private key from the fingerprint picture, which is then used to covertly store the user's credentials in an authentication server database. In the authentication step, we take a fresh picture of the user's biometric fingerprint, create the private key, and then encrypt the biometric information as a query. The authentication server receives the biometric data that has been queried and compares it to the data that has been stored there. The user is now prepared to access his or her service from the chosen server after successfully completing the authentication process. Mutual authentication utilising a short-term session key has been suggested between the user and authentication server as well as between the user and service server in order to achieve secure access to the service server. We describe an efficient and reliable method to create the session key using two fingerprint data. For message authenticity purposes, a biometric-based message authenticator is also created.

The essential contributions and advantages of the proposed strategy are outlined below.

1. A practical method for sending a user's biometric information to an authentication server through unencrypted network channels is given.
2. We provide a method for creating an irreversible fingerprint image straight from a revocable private key. The private key and a direct representation of the user's biometric information don't need to be kept anywhere.
3. By eliminating the need for the user's credentials to be kept on the authentication server, we overcome the drawback of conventional techniques.
4. We provide a unique technique for creating session keys.
5. Each entity needs some preloaded information in a typical authentication system, which adds overhead.

2. LITERATURE REVIEW

For security reasons, it is necessary that neither the client nor the server understand anything about the database or the requested biometry and the results of the matching procedure. The proposed protocol by Barni et al. [1] uses homomorphic encryption as the primary cryptographic primitive and adopts a multi-party computing strategy. Finger code, a specific encoding of fingerprint pictures, is used to reduce protocol complexity as minimal as feasible. Our main solution is a generic identification protocol and it allows to select and report all the enrolled identities whose distance to the user's finger code is under a given threshold, in contrast to previous works on privacy-preserving biometric identification that concentrate on choosing the best matching identity in the database.

It is a difficult task to implement closest neighbor request over encrypted data in the cloud while safely resisting the collusion of cloud server and query consumers. CloudBI-II has recently been proposed by Evans et al. [2] to facilitate closest neighbor queries on encrypted cloud data and is advertised as secure even when cloud servers conspire with certain untrusted query consumers. In this research, we suggest an effective attack strategy that predicts Cloud BI-II will expose the collusion attack's difference routes. The process of searching a pre-established biometric database for a matching record for an inquiring

ISBN - 978-93-95038-50-8

biometric attribute obtained from an unknown subject of interest is known as biometric identification (BI). Cloud computing, which offers many conveniences but also raises new privacy problems, has lately helped with this. Wang et al. [3] recently introduced two cloud-aided BI strategies that aim to protect privacy in ESORICS '15. In order to expose the security flaws in these two systems, we suggest various intricately designed attacks in this work. Theoretical analysis is provided to support our suggested assaults, and it shows that using such attacks, the cloud server may precisely deduce the external database and the identification request.

Furthermore, we demonstrate how the difference vector disclosure will lead to a major privacy violation and achieve a successful attack strategy to undermine CloudBI-II. That is, CloudBI-II is unable to provide the security that was promised. The proposed strategy can quickly retrieve the original data from the encrypted data set in CloudBI-II proposed by Zhu et al. [4] through theoretical analysis and laboratory assessment. Finally, we offer an improved system that effectively counters the collusion attack.

A password-based user authentication system for wireless networks of sensors was created by Jiang et al. [7] (WSNs). This kind of authentication uses both a smart card and a password, making it a two-factor method. An authorized user registers or reregisters with the trusted gateway node during the user signup process (GW N). The appropriate credentials are subsequently saved on a smart card that the GW N then provides. Additionally, all of the deployed sensor nodes register with the GW N using a secure channel and receive their corresponding secret credentials. During the login and verification phases, the GW N assists a genuine user in authenticating with a chosen sensor node using the pre-loaded credentials.

Other user authenticated based consensus strategies were put out by Turkanovic et al. [8]. However, the system developed by Turkanovic et al. [8] is vulnerable to assaults such as contactless payment theft, guessing offline login credentials, user impersonating, offline identification guessing, and sensor network impersonation [6]. A smart card-based user identification system that protects user privacy and employs hashing operations for biometric verification was created by Park et al. [9]. The plan, however, is vulnerable to denial-of-service (DoS) assaults [10].

A biometric-based user verified key agreement system was created by Pan et al. [5] for safe access to services offered by Internet of Things (IoT) devices. Despite using lightweight operations, this technique is not immune to DoS assaults since it employs the perceptual hashing (bio hashing) procedure rather than the fuzzy extractor used by [12]. This is largely due to the fact that the bio hashing approach seldom ever generates a particular feature BH(BIOi) from the physiological biometric BIOUi of an authorized user Ui at various input times, despite the fact that it may minimise output error [12]. There were several biometric applications developed by Gowroju et al. [16-21] that deals with security related applications efficiently using pupil of the person.

We may access shared configurable resources like memory, network, servers, services, and apps using the cloud-based solution instantly, conveniently, and from any place. Due to the numerous advantages that cloud platforms provide, many businesses are transferring and integrating their identity verification management systems there. Compared to on-premises biometric solutions, cloud biometrics are simpler to implement. Cloud-based biometrics solutions may be quickly integrated with any current online or desktop application via API integration.

ISBN - 978-93-95038-50-8

4. RESEARCH METHODOLOGY

We provide a reliable and privacy-preserving biometric identification system that can withstand a cloud and user-launched collusion assault. Our primary contributions, namely, may be summed up as follows: We analyses the biometric identification system and demonstrate its shortcomings and security flaws when exposed to the suggested level-3 attack. In particular, we show that the attacker may decode all users' biometric features by collaborating with the cloud to obtain their secret keys. We introduce a brand-new, effective biometric identification system that protects user privacy. The extensive security study demonstrates that the suggested approach is capable of achieving the necessary level of privacy protection. In particular, our system can withstand the suggested attack and is secure under the biometric identification outsourcing model as shown in Figure 1.

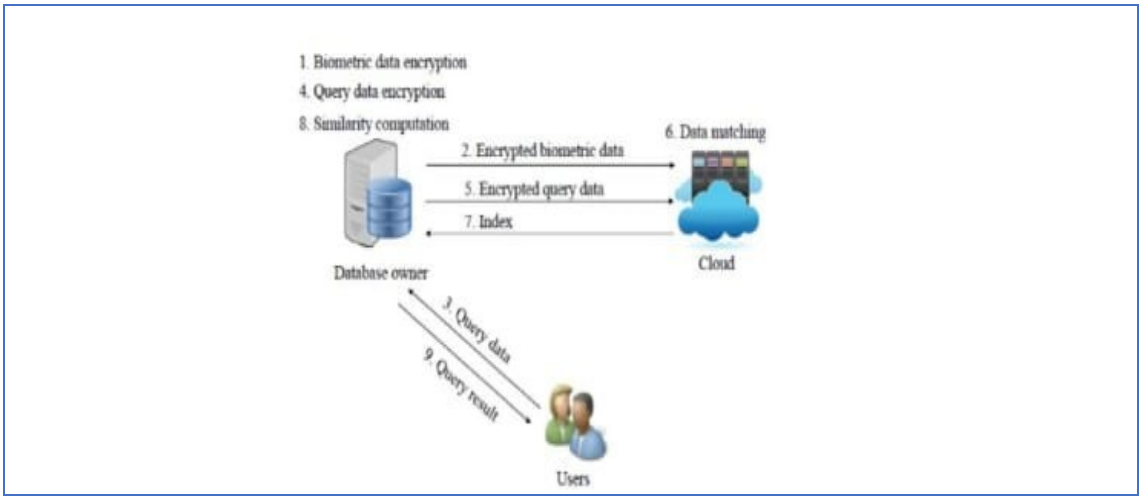


Figure 1: Architecture of Proposed system

In this study, we adhere to the widely used "Dolev-Yao (DY) threat model" [13]. The DY model allows an adversary, say A, to edit, remove, or even insert fake information into the messages as they are being sent. Communications exchanged while network elements are in communication. As a result, under the DY model, the network entities communicate with one another over a public channel. We also assume that while the authentication servers (AS) and resource servers (RS) are semi-trusted network entities, the clients are not. If low-entropy passwords are used in a password-based authentication scheme, password guessing attacks are possible. On the other hand, a brute-force attempt to guess biometric data in a biometric-based authentication method is computationally impossible. A, may, however, carry out further possible attacks, including replay, man-in-the-middle, privileged insider, denial-of-service, biometric data guessing, stolen smart card, and password guessing assaults (for password-based authentication schemes). Additionally, A has the ability to alter both stolen and previously stored biometric data.

When C receives a receive request, it first checks the received DB and remote DB to make sure the message is genuine. When the message is verified, C and remote server utilise session server for access to services. In this manner, C can use a service provided by RS. Figure. 2 depicts a summary of the messages sent and received during the user authentication phase of the proposed approach.

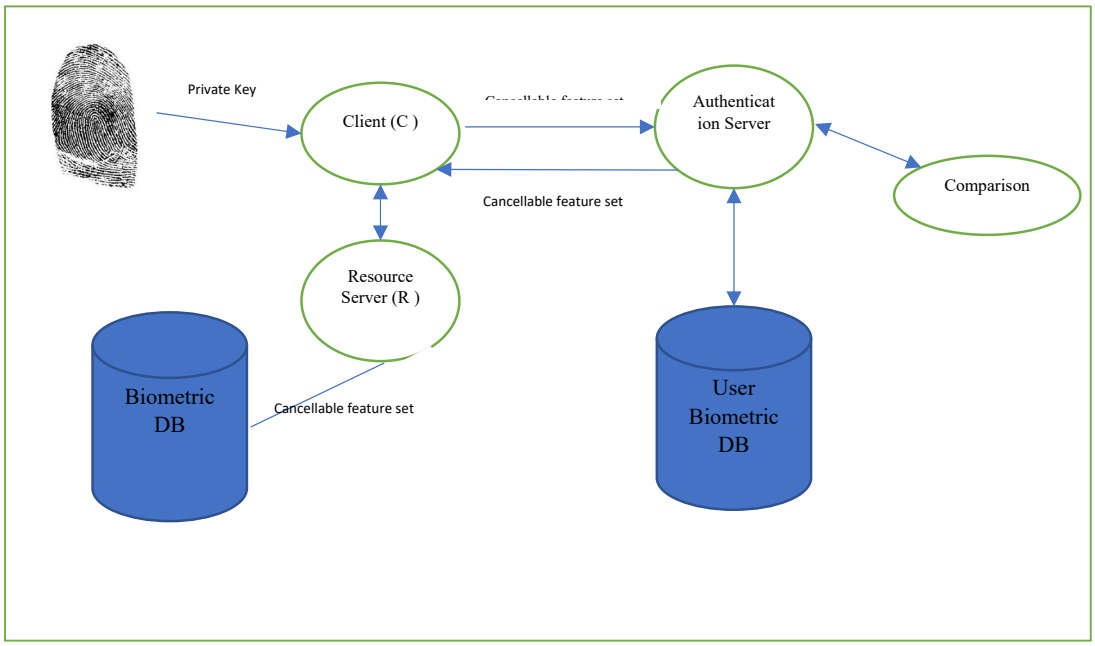


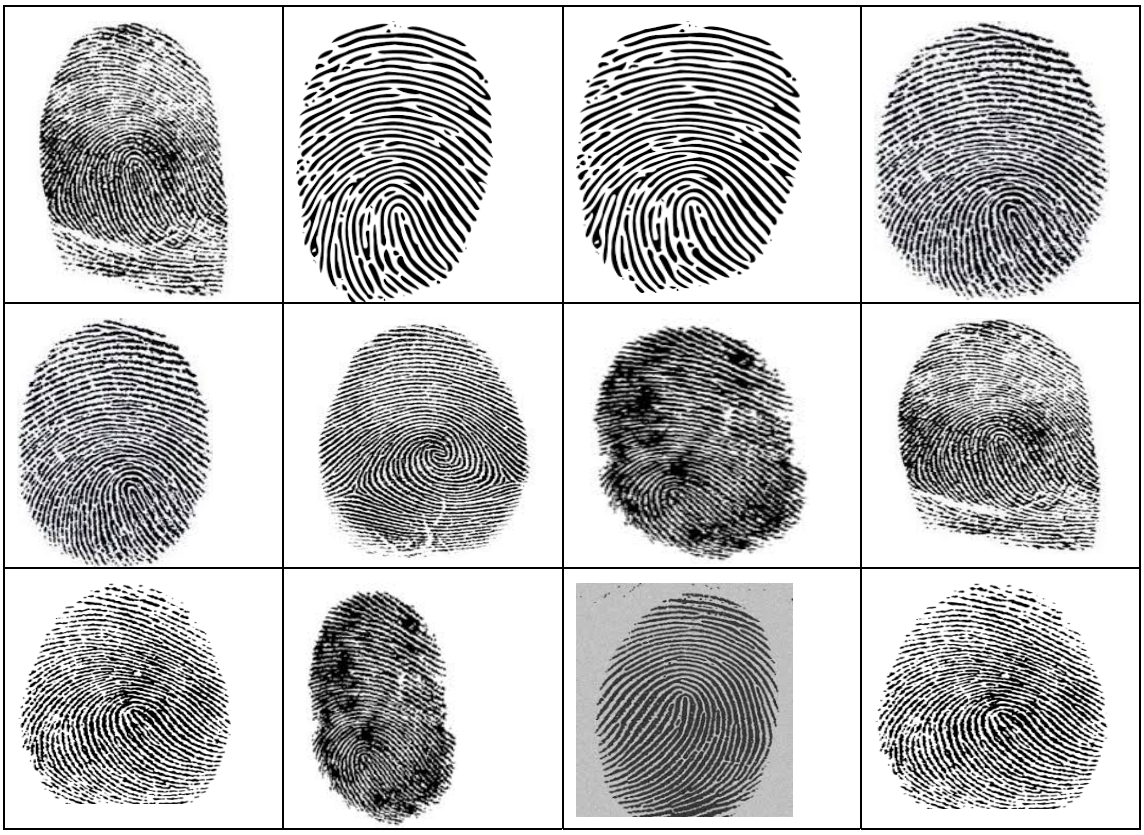
Figure 2: Authentication Mechanism

We extract every detail point from a user's fingerprint picture that has been taken. We initially align the fingerprint picture to improve feature extraction accuracy. We choose the consistent region from this fingerprint image that has been aligned. The fingerprint region, which has a high likelihood of appearing in any fingerprint picture that is recorded, can be described as the consistent region. To extract the minute points, we choose this constant region. We suggest using a horizontal segment to pick a group of minute points from the consistent region. A tiny portion of the consistent region, which has the most minute points, is represented by the horizontal segment. We choose these little details to create a codeword from the convolution coding's Trellis diagram.

This codeword shall be known as BioCode can then be used to create a private key, abbreviated Keyc. as Keyr is a random number, and Keyc = H(BioCode ⋈ Keyr) H is an application-generated standard hash produced by C. function and./ (for instance, Secure Hash Algorithm (SHA-1) [14]). is a one-way transformation of the two input parameters. It is much simpler to calculate in the forward direction, but not in a reverse fashion. Another option is SHA-256. [14] to make the suggested method very secure.

Proposed system uses publicly available dataset from [15]. A biometric fingerprint database called Sokoto Coventry Fingerprint Dataset (SOCOFing) was created with academic research in mind. 6,000 fingerprint photos from 600 African people make up SOCOFing, which also includes synthetically changed copies with three distinct levels of alteration for obliteration, central rotation, and z-cut. SOCOFing also includes labels for gender, hand, and finger names. The sample images from the dataset are shown in Table 1.

ISBN - 978-93-95038-50-8



5. Results and Discussions

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. Before registering into the application, it runs the PreCalcu procedure, and both C and AS have their current session keys, say K. C then does the following. The application of C records a fresh fingerprint picture of C, let's say Ireg. From Ireg, we take minutiae points and create minutiae pairs. We initially partition Ireg into a number of little square blocks in order to produce a pair of minutiae points (Figure.3). We go around each block in Ireg, creating pairs of minutiae points by taking into account that each minutiae point belongs to each block and that all minutiae points belong to its eight linked neighboring blocks. By moving through each block one at a time, we may create pairs of minute points. We determine the Euclidean lengths and angles of each of the obtained straight lines. Figure: shows the home page of authentication server.

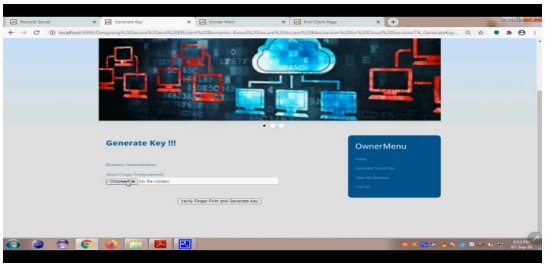


Figure 3: Authentication Server

ISBN - 978-93-95038-50-8

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 as shown in Figure 4. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server.

Figure 4: Generated key for individual user

To obtain secure access authentication mutually, between the user and authentication server, and also between the user and service server have been proposed using a session key as shown in Figure: 5. Using two fingerprint data, we present a fast and robust approach to generate the session key. First, we will be visiting the home page of the designing secure and efficient biometric based secure access. In this page we will be having cloud, owner, and user. In the home page when we click on the owner. This is the owner login page and we can login in to it by using password and username. If the owner is new, he /she can register by clicking on register as shown in Figure 6. once the owner is logged in, he/she will be asked for biometric finger print.

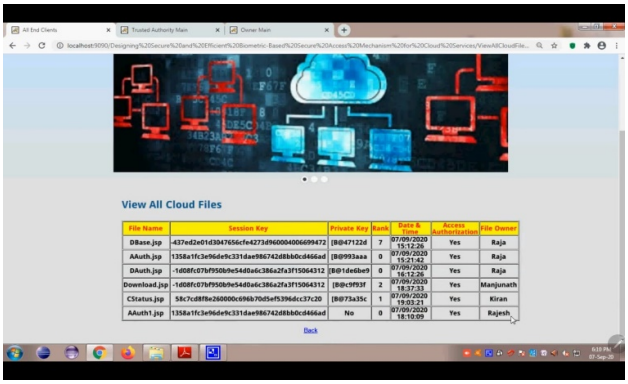


Figure 5: Access authentication of individual user

This is the owner main page where we can upload the images. In the upload images we need enter the title that we are going to upload and biometric image name that going to upload and you can add the biometric description to that image if needed. This is the user page where we can upload the images. In the upload images we need enter the title that we are going to upload and biometric image name that going to upload and you can add the biometric description to that image if needed. We need to put the biometric fingerprint to

login. This is the user main page as shown in Figure: 7 where we need to enter the keyword to search what the owner had uploaded.

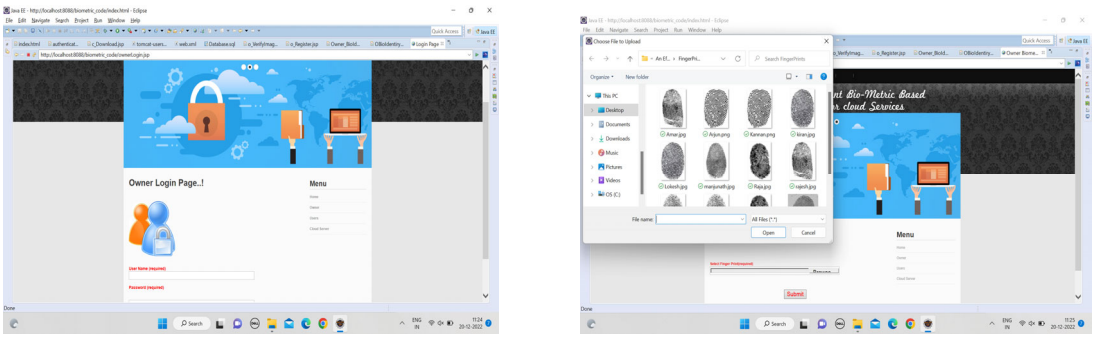


Figure 6: Login page and process of uploading finger print

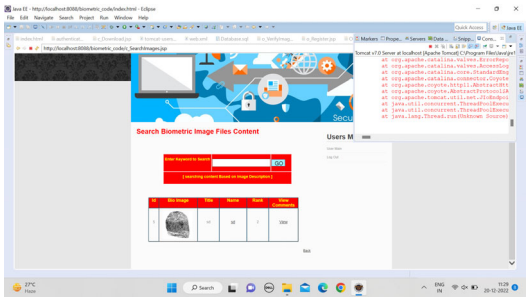


Figure 7: View of user

We create minutiae pairings by taking into account a core point and each minutiae point that is a part of the eight blocks that surround the identified core point (Figure. 3(b)). In a similar manner, we choose each minute point from the eight linked blocks that surround the block where the delta point is discovered (Figure. 8). We determine the Euclidean distances and angles for each pair produced using the core point and delta point. The delta point on a friction ridge is the location at or closest to the point of divergence of two type lines and is regarded to be a pattern of a fingerprint in biometrics and fingerprint scanning. when we tap on the name we will be getting to enter the file name and then we need to generate a private key. So that we can download the content that has been sent by owner.

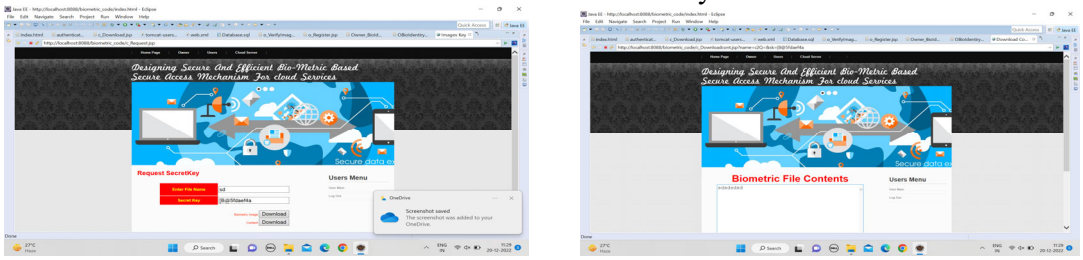


Figure 8: Biometric content viewer

This cloud server page. We just need to login. There is no need to register. It analyses owners list, users list, etc. These are the contents of the cloud server. Cloud can also see the

owner bio image files in the cloud services. Cloud can view owner and user as shown in Figure: 9.

Figure 9: Cloud view of existing users

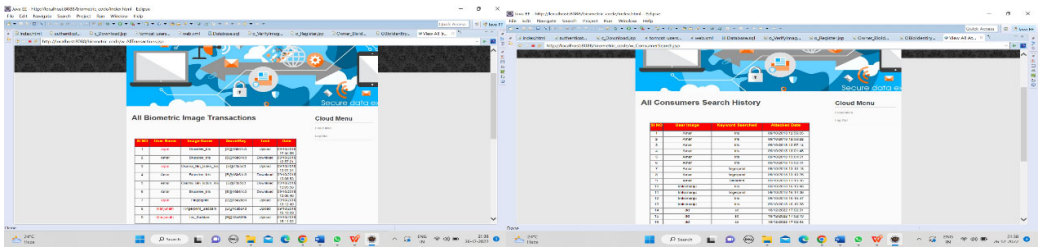


Figure 10: Admin view of the proposed system

If an adversary A has the biometric data of a legitimate user, may they utilise it to get secret information. This is due to the tampering attacks against stolen and stored biometric information (i.e., session key). A privileged-insider attack occurs when a trusted user acts as a privileged insider within the company to steal a registered user's secret credentials during registration, then makes an effort to utilise those stolen credentials. In the replay attack, A

tries to record the communications that are sent and then deceive another legal entity by using the information again when the two parties are communicating as shown in Figure:10.

A might try to update, edit, or delete the message contents that were sent to the receivers under the man-in-the-middle attack by listening in on communications between the entities.

If an attacker A with a stolen or lost smart card belonging to a registered user can extract all the credentials from its memory using power analysis techniques [14], they will next try to determine the user's secret credentials. An event that prevents a system or network from carrying out its anticipated functionality, such as resource depletion, is referred to as a denial-of-service (DoS) assault. In an impersonation attack, the adversary pretends to be the sender so that the receiver thinks the communication has come from a trustworthy source. If a password-based system is employed, adversary A could utilise eavesdropped communications, data kept in the system, and/or a user's smart device to attempt to guess a lawful user's password as shown in Figure: 11 (in either an online or offline mode).

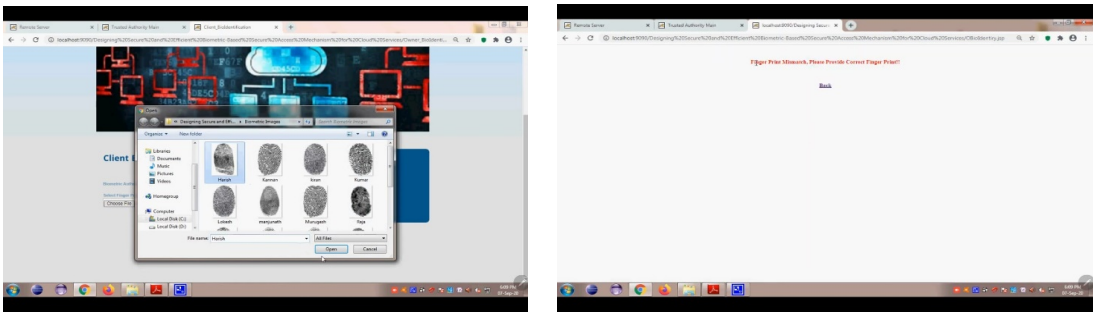


Figure 11: Attacker view of the proposed system

It has been found that the proposed system offers improved security for the biometric template maintained on the server, as well as user-generated private keys. Additionally, in contrast to current technology. It does not require a password or smart card for authentication techniques. The proposed system offers validity and strength for practical deployment in real-world applications as a consequence.

6. CONCLUSIONS

The growing use of biometrics demonstrates that it offers distinct benefits over traditional password and token-based security systems (e.g., on Android and iOS devices). In this research, we present an authentication method based on biometrics for users attempting to access services and computing resources from a distance. Our suggested method makes it feasible to build a private key from a fingerprint biometric reveal since it is able to do so with 95.12% accuracy. There is no need to communicate any prior information when utilizing the session key creation method, we suggest using two biometric data. Our strategy is more resistant to various known attacks when compared to other authentication methods of a similar nature.

ACKNOWLEDGEMENTS

This guideline and template are modified and tailored for SASAT-2023.

REFERENCES

1. Barni, Mauro, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, Dario Fiore et al. "Privacy-preserving fingercode authentication." In *Proceedings of the 12th ACM workshop on Multimedia and security*, pp. 231-240. 2010.
2. Evans, David, Yan Huang, Jonathan Katz, and Lior Malka. "Efficient privacy-preserving biometric identification." In *Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS*, vol. 68, pp. 90-98. 2011.
3. Wang, Lizhe, Jie Tao, Marcel Kunze, Alvaro Canales Castellanos, David Kramer, and Wolfgang Karl. "Scientific cloud computing: Early definition and experience." In *2008 10th ieee international conference on high performance computing and communications*, pp. 825-830. Ieee, 2008.
4. Zhu, Youwen, Yue Zhang, Xingxin Li, Hongyang Yan, and Jing Li. "Improved collusion-resisting secure nearest neighbor query over encrypted data in cloud." *Concurrency and Computation: Practice and Experience* 31, no. 21 (2019): e4681.
5. Pan, Shiran, Shen Yan, and Wen-Tao Zhu. "Security analysis on privacy-preserving cloud aided biometric identification schemes." In *Australasian Conference on Information Security and Privacy*, pp. 446-453. Springer, Cham, 2016.
6. W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "NIST Special Publication 800- 63-2: Electronic Authentication Guideline," 2013, National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Accessed on July 2019.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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
12. 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.
13. 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.
14. "Secure Hash Standard," FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Accessed on January 2019.
15. Gowroju, Swathi, and Sandeep Kumar. "Robust Deep Learning Technique: U-Net Architecture for Pupil Segmentation." *In 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0609-0613. IEEE, 2020.
16. Swathi, Aarti, and Sandeep Kumar. "A smart application to detect pupil for the small dataset with low illumination." *Innovations in Systems and Software Engineering* (2021): 1-15.
17. Swathi, Aarti, and Sandeep Kumar. "Review on Pupil Segmentation Using CNN-Region of Interest." In *Intelligent Communication and Automation Systems, pp. 157-168. CRC Press*, 2021.
18. Gowroju Swathi, Aarti and Sandeep Kumar. "Robust Pupil Segmentation using UNET and Morphological Image Processing." In 2021 *International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, pp. 105-109. IEEE, 2021.

19. Swathi, S. Kumar, V. S. T, S. Rani, A. Jain and R. K. M.V.N.M, "Emotion Classification using Feature Extraction of Facial Expression," 2022 2nd *International Conference on Technological Advancements in Computational Sciences* (ICTACS), 2022, pp. 283-288, doi: 10.1109/ICTACS56270.2022.9988544.
20. Swathi Gowroju, Sandeep Kumar, Aarti, Anshu Ghimire, "Deep Neural Network for Accurate Age Group Prediction through Pupil Using the Optimized UNet Model", *Mathematical Problems in Engineering*, vol. 2022, Article ID 7813701, 24 pages, 2022. https://doi.org/10.1155/2022/7813701