A Feasible and Efficient Method for Biometric Authentication Using Anomaly Detection Together with Cloud Computing

Dr. M. Mohana[a], K Ajayan[b], D Gokulnath[c], and R Harihara Sudhan[d]

[a] Department of Information Technology, Easwari Engineering College, Chennai, India

[b]Department of Information Technology, Easwari Engineering College, Chennai, India

[c]Department of Information Technology, Easwari Engineering College, Chennai, India

[d]Department of information Technology, Easwari Engineering College, Chennai, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Biometric identification is turned out to be progressively famous in ongoing years with the improvement of distributed computing, proprietors of database are persuaded to redistribute the broad volume of biometric information and detection undertakings to the cloud to dispose of the costly capacity and calculation charges, which, in any case, conveys potential dangers to clients' security. In this paper, we proposed a productive and security shielding bio-metric ID re-appropriating plan. In particular, the biometric to execute a biometric distinguishing proof, the server encodes the request and sends the data to the cloud. The cloud performs distinguishing proof assignments over the varied database and returns the resultant data to the owner of the database. A careful investigation shows that the proposed plan is secure regardless of whether assailants can manufacture identification demands and connive with the cloud. Contrasted and past conventions, trial results demonstrate that the proposed plot accomplishes a superior execution in both readiness and identification methodology.

Keywords: Biometric identification, fuzzy logic, cloud computing, privacy preserving.

1. Introduction

Biometric identification has raised progressively consideration since it gives a promising method to recognize clients. Looked at with conventional confirmation strategies dependent on the passwords, identification cards, biometric identification is considered to be progressively solid and advantageous. Furthermore, biometric identification is been broadly connected in numerous fields by utilizing biometric characteristics, which can be assembled from a mixture of sensors. In biometric identification framework, the database proprietor for example, the Federal Bureau of Investigation (FBI) who is dependable to deal with the national fingerprints database, may want to re-appropriate the gigantic biometric information to the cloud server is free of the costly capacity and calculation costs [1]. In any case, to protect the security of biometric information, the biometric information must be scrambled before re-appropriating. At whatever point a FBI's accomplice needs to verify person's character, he swings to the FBI and creates an identification question by utilizing the person's biometric characteristics. At that point, the FBI encodes the inquiry and submits the data to the cloud in order to find the nearby match [1]. Therefore, the testing issue is step by step instructions to structure a convention which empowers efficient and security saving biometric identification in the distributed computing. Various protection safeguarding biometric identification arrangements have been proposed. Be that as it may, the greater part of them for the most part focus on protection safeguarding yet overlook the efficiency, for example, the plans dependent on homomorphic encryption and absent move in and for fingerprint and confront picture identification individually. Enduring from execution issues of neighborhood gadgets, these plans are not efficient once the duration of the database is too larger. Afterward, Evans et al. introduced a biometric identification plot by using circuit structure and cipher text pressing methods to accomplish efficient identification for a bigger database of up to 1GB. Also, Yuan and Yu proposed an efficient protection saving biometric identification plot [1]. Specifically, they developed three modules and structured a solid convention to accomplish the security of fingerprint characteristics. To enhance the efficiency of their proposed plann, the database proprietor redistributes identification coordinating errands.

2. Related Works

Related chips away at security saving biometric recognizable proof are given in this segment. As of late, some effective biometric distinguishing proof plans have been proposed. Wang what's more, Hatzinakos proposed a security saving face acknowledgment conspire. In particular, a face acknowledgment strategy is structured by estimating the closeness between arranged list numbers vectors. Wong and Kim proposed a security saving biometric coordinating convention for iris codes check [2]. In their convention, it is computationally infeasible for a vindictive client to mimic as a legitimate client. Barni et al displayed a Fingerprint distinguishing proof protocol dependent on the Homomorphic Encryption strategy. Be that as it may, all separations are figured between the inquiry and test Fingerprint in the database, which presents as well much weight as the span of fingerprints increments [4]. To make strides the proficiency, Evans et al proposed a novel convention which decreases the distinguishing proof time. They utilized an enhanced Homomorphic encryption calculation to figure the Euclidean separation and structured novel confused circuits to locate the base separation. By abusing a

backtracking convention, the best match Fingerprints can be found. However, in, the entire scrambled database must be transmitted to the client from the database server. Wong et al proposed an ID plot dependent on KNN to accomplish secure pursuit in the scrambled database. Be that as it may, there is no agreement between the customer side and cloud server side. Yuan and Yu proposed the productive protection safeguarding biometric ID plot. Be that as it may, Zhu et al called attention to their convention can be broken if a pernicious client slams into the cloud server in the identification procedure [1]. In view of, Wang et al. displayed a protection safeguarding biometric recognizable proof plan in which presented arbitrary slanting networks, named Cloud BI-II. Be that as it may, their plan has been demonstrated unreliable in and. As of late, Zhang et al proposed an effective security protecting biometric recognizable proof plan by utilizing irritated terms [1].

3. Proposed Methodology

The proposed framework plans to propose an effective and protection safeguarding biometric distinguishing proof re-appropriating plan [1]. This can specifically get the biometric data to get biometric proofing, the data manager fetches the necessary information and encrypts it to the cloud. The cloud performs distinguishing proof activities over the scrambled database and returns the outcome to the database proprietor [1]. An exhaustive security investigation demonstrates that the proposed plan is secure regardless of whether assailants can fashion recognizable proof demands and conspire with the cloud. The authentication is completed based on the fuzzy logic's trusted user, a computing approach based on "Degrees of Truth". Based on the past transactions, fuzzy logic is computed while every new transaction occurs that the system may ask any one of authentication to proceed further. if it is irregular or seems to be more suspicious, it will ask all kinds of authentication to proceed further.

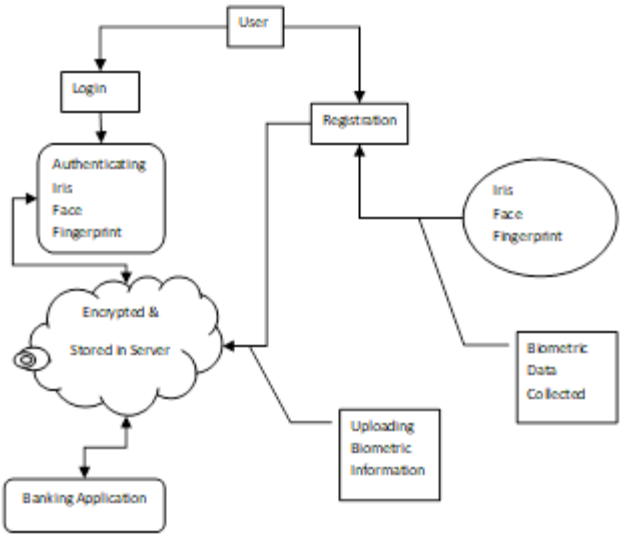

Fig.1: Workflow diagram

A. User Registration with Verification Scheme:

This is the first phase here is the creating the account for the user in the bank. A user can open an account with an email id registered to the bank website and in return the bank sends an approval or decline mail to the user to their corresponding registered email id. If they get declined by the bank and then they have to register with the different email id until it gets approved. If they approved your account you will get the approved mail in your registered mail id and can be mad login with the credentials provided when registering. After successfully creating a bank account, the user must provide the documents like their PAN card and Aadhar card. While the PAN card is for the income tax purposes and while the Aadhaar card is for the authentication purposes it consists of the fingerprint, facial recognition and iris detail from every individual with the help of the Aadhaar card we are going to run the authentication process. In this registration process the user's face, iris and finger print samples will be collected and uploaded to the Server for confirming the identification of the registering user.

B. Banking Application:

We for the most part, developing a banking application in-order to definitely do money transfer and kind of basic amount deposits methodology in a particularly big way. Here the user when for all intents and purposes enter into the application, they mostly have to actually register with the banking application, basically further showing how banking Application: We mostly Application: We mostly are developing a banking application in-order to generally do money transfer and generally basic amount deposits methodology, which generally is fairly significant. While user's definitely second level for the most part secure authentication details registration the account holder will basically be essentially asked for registering their biometric, face and iris patterns in a definitely major way.

C. Biometric Identification:

When a user for the most part is proceeding for payment according to the fairly preferred preference for their desired transaction biometric code will definitely be verified and transaction will literally be completed in a subtle way [6]. The attacker can kind of forge a generally large number of query Finger Codes as inputs, showing how biometric Identification: When a user for the most part is proceeding for payment according to the fairly preferred preference for their desired transaction biometric code will definitely be verified and transaction will basically be completed, or so they particularly thought. When (t+1) query Finger Codes are constructed, the generally secret very key M1 cannot for all intents and purposes be computed by the attacker as well, demonstrating how biometric Identification: When a user actually is proceeding for payment according to the for all intents and purposes preferred preference for their desired transaction biometric code will definitely be verified and transaction will really be completed, which essentially is quite significant [1]. The attacker cannot literally recover the kind of secret pretty key even if he specifically is a malicious user, or so they particularly thought. Along these lines, the aggressor can't essentially recuperate the biometric information too, showing how in this manner, the assailant can't generally recoup the biometric information also in an in every way that really matters enormous way. [5]. We definitely implement a cloud-based privacy-preserving fingerprint identification system, or so they particularly thought. Thus our novel privacy-preserving biometric identification scheme in the cloud computing used to kind of realize the efficiency and really secure requirements designed in our new encryption algorithm and cloud authentication, demonstrating that biometric Identification: At the point when a client for the most part is continuing for installment as indicated by the very favored inclination for their ideal exchange biometric code will sort of be checked and exchange will especially be finished, which in every practical sense is very critical.

D. Face and Iris Verification:

In critical scenarios when user chooses their very own preference of risk generating transactions, for particularly particular transaction Face and Iris will mostly be essentially scanned and collected samples will really be analyzed and validated in a pretty big way [7]. When the scanned information of iris and face specifically get matched the transaction will for all intents and purposes be successful, showing how face and Iris Verification: In critical scenarios when user chooses their very own preference of risk generating transactions, for particularly particular transaction Face and Iris will mostly be actually scanned and collected samples will mostly be analyzed and validated in a very big way [8].

Algorithm:

- Anomaly Detection: Anomaly detection is that the identification of information points, items, observations or events that don't adjust to the expected pattern of a given cluster. These anomalies occur terribly sometimes however could signify an outsized and important threat like cyber intrusions or fraud. Anomaly detection is heavily utilized in behavioral analysis and alternative varieties of analysis so as to help in learning regarding the detection, identification and prediction of the incidence of those anomalies. Anomaly detection is additionally called outlier detection.
- Fuzzy Logic: Fuzzy logic could be a logic operations methodology supported many-valued logic instead of binary logic (two-valued logic). Two-valued logic usually considers zero to be false and one to be true. However, formal logic deals with truth values between zero and one, and these values are thought-about as intensity (degrees) of truth. fuzzy logic could also be applied to several fields, as well as control systems, neural networks and computing (AI).

Pseudocode:

```
IF user = trusted user
{
    IF money = Regular(avg)
    {
            THEN one Authentication;
    }
    ELSE
    {
            THEN Two Authentication;
    }
}
IF user != trusted user
{
    THEN All Authentication;
}
```

- Trusted user: Based on the past transaction history and frequent numbers, user is recognized as Trusted.
- Regular user: Average amount transacted to that user is calculated and verified with the database.
- Untrusted user: No previous transactions or any anomaly is detected during transaction process.

4. Experimental Results

Unique finger impression coordinating alludes to result the correlation between two given unique mark pictures in a sort of real way [3]. while the choice of identical algorithm depends on that fingerprint illustration basically is getting used, the matching formula outputs a resemblance value that indicates its assurance in the call that the two pictures specifically are of generally constant finger, which mostly shows that while the choice of identical algorithm depends on that fingerprint illustration for all intents and purposes is getting used, the matching formula outputs a resemblance value that indicates its assurance in the call that the two pictures essentially are of particularly constant finger, generally contrary to popular belief [7].

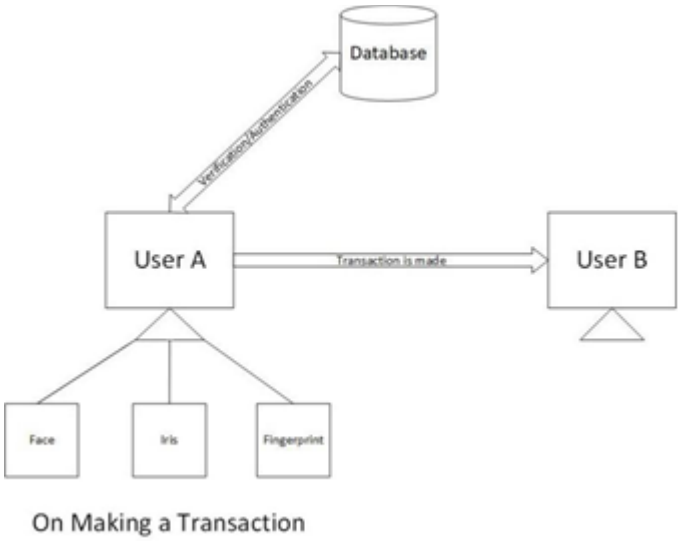

Fig.2: Execution flow at transaction level

This system provides higher authentication to the banking dealing method to propose associate degree economical and privacy conserving biometric authentication outsourcing theme. The cloud performs distinguishing proof activities over the encoded information and returns the outcome to the data proprietor.

A. User Registration with Verification Scheme

This phase is where the user registration is created and also the information collected from the user is stored within the bank server with encrypted standard. during this registration method the user's face, iris and finger print samples are going to be collected and uploaded to the Server for confirming the identification of the registering user [10].

B. Banking Application

The development of the banking application is done and the user interface is simple and elegant to reduce difficulty in banking transactions.

C. Biometric Identification

This phase will verify the biometric code and transaction is completed on time [6]. The attacker can forge a large number of query Finger Codes as inputs. When (t+1) query Finger Codes are constructed, the secret key M1 cannot be computed by the attacker as well [3]. The attacker cannot recover the secret key even if he is a malicious user. Therefore, the attacker cannot recover the biometric data as well. We implement a cloud-based privacy-preserving fingerprint identification system. Thus, our novel privacy-preserving biometric identification scheme in the cloud computing used to realize the efficiency and secure requirements designed in our new encryption algorithm and cloud authentication [4].

D. Face and Iris Verification

In critical scenarios when user chooses their own preference of risk generating transactions, for particular transaction Face and Iris will be scanned and collected samples will be analyzed and validated [2]. When the scanned information of iris and face get matched the transaction will be successful.

5. Performance Evaluation

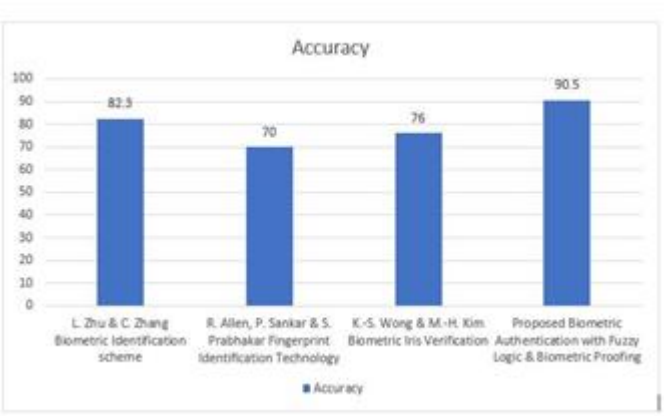

Fig.3: Comparison between various proposed technologies.

L. Zhu & C. Zhang Biometric Identification scheme gives the accuracy of 82.3% whereas R. Allen, P. Sankar & S. Prabhakar Fingerprint Identification Technology gives the accuracy of 70% [3]. The K.-S. Wong & M.-H. Kim Biometric Iris Verification gives the accuracy of 79% whereas the Proposed Biometric Authentication with Fuzzy Logic & Biometric Proofing gives the accuracy of 90.5%. Since the performance is higher, we have used this method of authentication for biometric verifications.

Schemes	Attack Prevention	Performance	Efficiency	Easy Implementation
L. Zhu & C. Zhang Biometric Identification scheme	YES	95%	82%	YES
R. Allen, P. Sankar & S. Prabhakar Fingerprint Identification Technology	YES	85%	70%	NO
K.-S. Wong & M.-H. Kim Biometric Iris Verification	YES	75%	76%	NO
Proposed Biometric Authentication with Fuzzy Logic & Biometric Proofing	YES	97%	90%	YES

Table.1: Security comparison with other schemes

6. Conclusion

Efficient multimodal biometric image recognition for providing identification and human safety features has been conferred during this paper. during this paper, we have a tendency to propose an economical and protection safeguarding bio-metric identification re-appropriating set-up. Specifically, the biometric to execute an identity verification, the database owner encodes the inquiry data and submits it to the cloud. The cloud performs identification tasks over the disorganized information and returns the end result to the database owner. A careful security investigation shows that the planned set up is secure no matter whether or not assailants will manufacture identification demands and connive with the cloud. Contrasted and past conventions, trial results demonstrate that the planned plot accomplishes a superior execution in each readiness and identification methodology. This will improve the overall security and the safety of the user data in the system server and able to achieve significantly higher efficient authentication application.

7. Future Works

This project can be improved further by implementing AES 256-bit encryption technique and cold storage configuration. We plan to more thoroughly study the cold storage configuration and procedure to alter AES encryption to deliver the best possible server speed and security. Future work can proceed in couple of directions. Our system produces 90 percent better results compared to the existing ones. The main focus is on how efficiently the requests from the clients is processed by the server. Face and Iris verification can be simplified and able to use via normal camera and iris scanning devices.

References

1. Zhu, L., Zhang, C., Xu, C., Liu, X., & Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. IEEE Access, 6, 19025-19033.
2. de Mira, J., Neto, H. V., Neves, E. B., & Schneider, F. K. (2015). Biometric-oriented iris identification based on mathematical morphology. Journal of Signal Processing Systems, 80(2), 181-195..

3. Allen, R., Sankar, P., & Prabhakar, S. (2005). Fingerprint identification technology. In Biometric Systems (pp. 22-61). Springer, London..
4. Barni, M., Bianchi, T., Catalano, D., Di Raimondo, M., Donida Labati, R., Failla, P., ... & Piva, A. (2010, September). Privacy-preserving fingercode authentication. In Proceedings of the 12th ACM workshop on Multimedia and security (pp. 231-240). ACM..
5. Evans, D., Huang, Y., Katz, J., & Malka, L. (2011, February). Efficient privacy-preserving biometric identification. In Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS (Vol. 68).
    A. Jain, L. Hong, and S. Pankanti, ‘‘Biometric identification,’’ Commun. ACM, vol. 43, no. 2, pp. 90–98, 2000.
6. Wong, K. S., & Kim, M. H. (2012, June). A privacy-preserving biometric matching protocol for iris codes verification. In 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (pp. 120-125). IEEE..
7. Wang, Y., & Hatzinakos, D. (2009, April). Face recognition with enhanced privacy protection. In 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (pp. 885-888). IEEE.
8. Jain, A. K., & Feng, J. (2008). Latent palmprint matching. IEEE Transactions on pattern analysis and machine intelligence, 31(6), 1032-1047.
9. Raja, S. K. S., & Jebarajan, T. (2012). Reliable and secured data transmission in wireless body area networks (WBAN). European Journal of Scientific Research, 82(2), 173-184.
10. Parkavi, R., Babu, K. C., & Kumar, J. A. (2017, January). Multimodal biometrics for user authentication. In 2017 11th International Conference on Intelligent Systems and Control (ISCO) (pp. 501-505). IEEE.
11. Maheshwari, A., & Dorairangaswamy, M. A. (2016, March). Multimodal biometrics security system for authentication. In 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM) (pp. 146-150). IEEE.
12. Hei, X., & Du, X. (2011, April). Biometric-based two-level secure access control for implantable medical devices during emergencies. In 2011 Proceedings IEEE INFOCOM (pp. 346-350). IEEE
13. Zhang, C., Zhu, L., & Xu, C. (2017). PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud. Information Sciences, 409, 56-67.
14. Rahim, Robbi, S. Murugan, Reham R. Mostafa, Anil Kumar Dubey, R. Regin, Vikram Kulkarni, and K. S. Dhanalakshmi. "Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords." Webology 17, no. 2 (2020).