IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

# Enhancing Data Privacy through an Advanced Pseudonym System for Data Anonymization

**[1]Bammidi Swathi and [2]Panduranga Vital Terlapu**

[1] P.G Scholar, Department of Computer Science & Engineering, Aditya Institute of Technology and Management, Tekkali-532201,India ,bammidiswathi07@gmail.com

[2]Associate Professor, Department of Computer Science & Engineering, Aditya Institute of Technology and Management,Tekkali-532201, India. vital2927@gmail.com

## ABSTRACT

In biometric authentication, large amounts of data are stored on a database server and are accessed via wireless networks and cloud computing techniques. To access the data, we need a unique identification number; otherwise, the data will be authorised by a third party. To circumvent this, we've implemented a Pseudonym System that stores the data between the unique identifier and a biometric authentication method based on the palm vein. During the authentication process, data is stored in the database using anonymous methods and the binary format of pseudo-creation, which can provide a higher level of protection using binary vectors and master key vectors with random key generation to protect user privacy. Nowadays, data privacy and data storage are crucial in all organisations. Cloud Computing and other services are used to store the data. This reduces the time required to receive the result. The third party has no access to the data until he has obtained the unique identifier. Various methods of data anonymization and data privacy are employed here to protect the data.

**INDEX TERMS:** Authentication, palm vein, palm scanner, pseudonym, anonymity, data preservation, binary vectors, master vectors, and random key.

## I. INTRODUCTION

The amount of data that must be stored has grown exponentially in recent years. When we need to share data with third parties, we require data privacy to prevent unauthorised access to personal and confidential information. Despite the fact that some schemes have been developed, we continue to face data privacy issues. They use a single unique identification number or identity to protect the data and maintain the security of all the records; the

ISSN PRINT 2319 1775 Online 2320 7876
Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

records may be interconnected. This approach suggests verification mechanism for use in ICT that would protect the anonymity of senders. With this system in place, cars and computers need only make a single connection to a trustworthy authority to acquire confidential information, from which they can then create pseudonyms for verification on the recipient side [10]. Furthermore, [8] suggested an indirect reciprocity-based security 2 structure to regulate on-board VANET units' conduct, cut down on the number of possible assailants, and use the blockchain method to protect the image. This study focuses primarily on privacy protection through the use of a pseudonym system employing palm vein images.

## II. PROBLEM DEFINITION

Controllability is a disadvantage that may result from the application of widely accepted methods. As a result, data is readily accessible through a web of links, free from the shackles of censorship or regulation. Their system facilitates the management of information and the exchange of data in a secure environment. In conclusion, they have suggested that future specialists examine exhaustively the various techniques described in the literature for providing pseudonyms securely. In [3], researchers looked into the state of wireless sensing network data gathering while maintaining user anonymity. Using the most common privacy preservation methods, we contrasted and categorised existing data security consolidation strategies. Thus, the development of efficient protocols that do not rely on a trusted authority and secure two-way communication channels is necessary.

## III. OBJECTIVE OF PROJECT

The process of exchanging information. This paper proposes the use of a palm vein-based biometric authentication method during the authentication process as a means of mitigating such threats.

In addition, a pseudonym creation technique is utilised to make the database record anonymous, thereby ensuring that the data is adequately protected. Thus, unauthorised parties are unable to gain access to data/information. The proposed system is capable of resolving the leaked information, and the true identity of the user is never revealed to others.

## IV. EXISTING LITERATURE REVIEW SYSTEM

Literature is comprised of numerous approaches to data privacy preservation. Contrarily, the amount of data that needs to

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

be shared with external parties is increasing at an exponential rate and is used for a variety of purposes. It's also possible for malicious actors to gain access to sensitive information when people and organisations exchange data. Consequently, data privacy protection necessitates highly efficient and trustworthy methods.

In reference [8], three presently-utilized approaches were discussed. The three methods are de-identification, aggregated data that is protected from prying eyes, and processes on secured data. However, because of the inability to guarantee data privacy, these methods were considered impractical. However, they arrived at the conclusion that the de-identification strategy would be the most effective in terms of privacy protection if a highly effective and privacy-protective programme could be developed for that reason.

Several methods for keeping sensitive material secret have been created by different researchers, as reported in [13]. However, there is a lack of a definitive categorization for techniques that protect individual private.

In light of this, [13] classified methods for preserving data as either cryptography or non-cryptographic. However, enemies also make use of cutting-edge tools and regularly show off novel approaches to data and information theft in order to stay one step ahead of law enforcement. As a result, the critical need to create effective methods in this area was reaffirmed by [13]. Methods like palm prints, hand vein scans, fingerprints, and eye scans are all used in biometric identification systems.

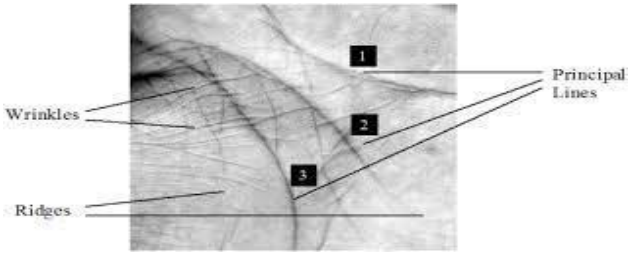


**Figure 1**: Palmprint Features

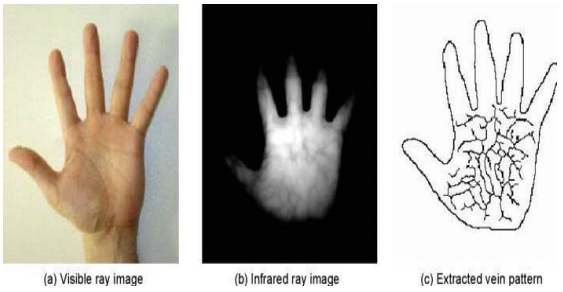


**Figure 2**: Features of Palm Vein

## V. PRESERVING DATA PRIVACY APPROACHES

In today's world, data has become more extensive, and we must share it with third parties for specific reasons; therefore, it must be kept private and secure. We need few approaches for this [16].

### A. Pseudonym System

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

By means of pseudonym systems, numerous users will interact with various organisations. Every organisation will be aware of one user with multiple pseudonyms, but these pseudonyms cannot be connected.

The procedure for using this system is:

**1. Master key generation**

Users and businesses alike must start by creating a master private key to go along with the master public key. Its main function is to decrypt incoming protected messages.

**2. Enrol with the CA organisation**

This CA organisation will maintain the identity of each user and is familiar with the master public key. If the user is dishonest, the CA is responsible for protecting the master key and master public key.

**3. Registration with an institution**

To generate a pseudonym, the user must contact the organisation, at which point the master key is extracted and the user can then contact the CA for credentials that were generated by the CA.

**4.The issuance of credentials**

Both the user and the organisation must be involved with credentials.

**5.Transfer of Credentials** After receiving the credentials, the user contacts the organisation to ensure their security. Here, the user's credentials are transferred from their pseudonym with one organisation to their pseudonym with another.

## VI. PROPOSED SYSTEM

In this project, we proposed to employ the pseudonym technique in order to protect the confidentiality of data by utilising palm vein. As was previously stated, hand vein is a trustworthy biological feature that can be used to create aliases. Homomorphic cryptography is used to create pseudonyms. To protect the privacy of user data, I implemented the same data anonymization techniques .

**1. Capturing Vein Image**

The palm vein scanner captures images of the veins. The documents are scanned and extracted from the database. Taking palm vein image as input.

**2. The Filtering of Images**

The filtering tools are utilised for image filtering and data filtering to improve quality. It is also for noise reduction. Utilizing the CLAHE filter to acquire minute points.

**3. Limit Detection**

Using the Canny edge detector, detect the image's boundary. It is primarily utilised for examining vein patterns. We employed the Guassian smoothing filtering method to

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

eliminate the noise[17]. Using sobel filters to apply Canny edge detection.

**4. Feature Important Facts**

Here, we are employing the Harris method to extract key points. Euclidean Distance [15] will be computed using these key points and the original palm image.

**5. Data Anonymization**

It is used to protect the confidentiality of data. With the pseudonym, we are able to determine who signed a message using their private key.

**6. Biometric key generation as Master key**

A biometric key is created from the collected feature keys, and this becomes the primary encryption key. After the function is recovered and the lines are chosen as critical feature points, the hand vein picture matrix is used to calculate the Euclidean distance metric. In the plane of m and n, the expression

$$d^2(m,n) = (m_1 - n_1)^2 + (m_2 - n_2)$$

**Data For Binary Value Master Key Generation**

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 |

Result: User will recognize the data from the above sample data.

| | |
|---|---|
| Master key generation from Binary vector | 326239370 |
| Random Data user id | 102012017 |

**Figure 3**:Biometric Key Generation As Master Key

**7. Pseudonym**

Extract 30 points from each row of an image, and then normalise those points to obtain binary values of 0 and 1. Convert binary to decimal to obtain the master key. Key points and random username values are used to generate two values, which are then merged to produce HMAC-SHA256. PSEUDONYM. To generate a pseudonym, HMAC-SHA256 accepts two inputs, such as a master key and merged values.

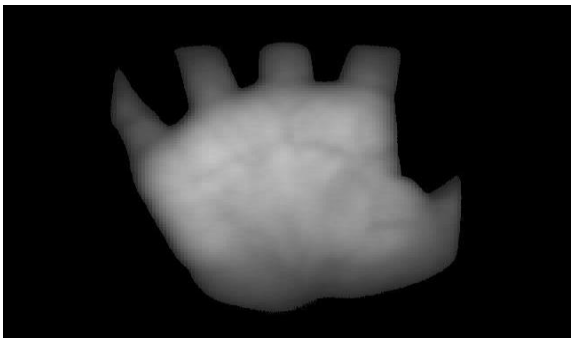

**Figure 4**: Palm Vein Image

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

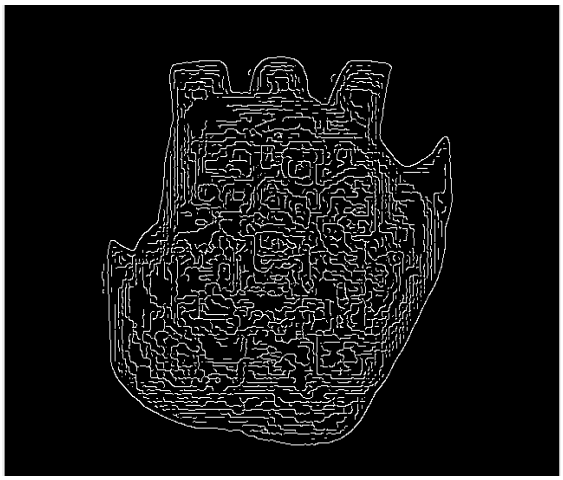

**Figure 5**: Palm Scanning To Extract Feature Points

## VII. PROPOSED METHODOLOGY

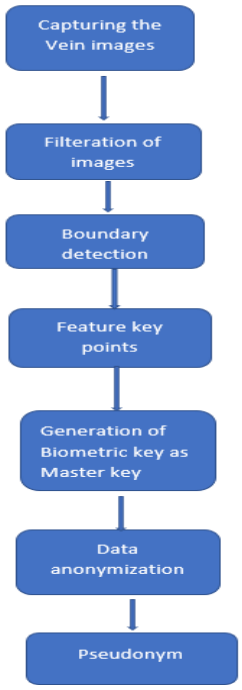


**Figure 6**: Process for preserving data

8. We have designed two modules for project implementation.

**i. Register module:** utilising this module, we will enter a username, a message, and a palm vein image as input, then apply the above nine points to generate a PSEUDONYM, and then upload these values to the DRIVEHQ cloud.

**ii. Recognition Module:** We will input the username and palm vein image, and then the application will generate a pseudonym that will be compared with the DRIVE HQ pseudonym. If both pseudonyms match, the user will be authenticated and only their message will be displayed.

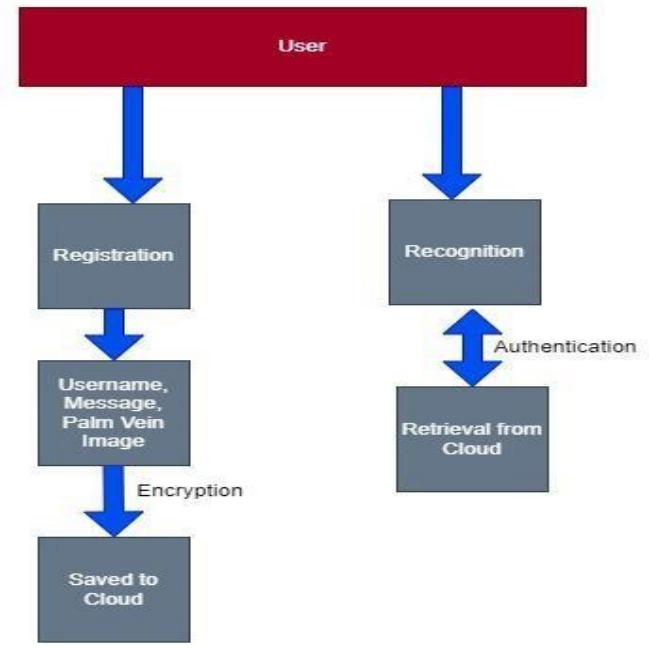


**Figure 7**. Proposed System Architecture

## VIII. ADVANTAGES AND DISADVANTAGES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

| Biometric Method | Advantage | Disadvantage |
|---|---|---|
| Finger print | 1. For every person it is different pattern.<br>2. Easy to use and it is highly accurate<br>3. Less space storage | 1. Usually<br>their fin<br>everywh<br>2. Less qua |
| Palm print | 1. For every person it is different pattern.<br>2. We don't use palm print everwhere compared to fingerprint. | Less quality of |
| Palm vein | 1. For every person it is different pattern.<br>2. We cant see directly by eyes.<br>3. Have unique features<br>4. More secure and accurate compared to both. | Database is us |

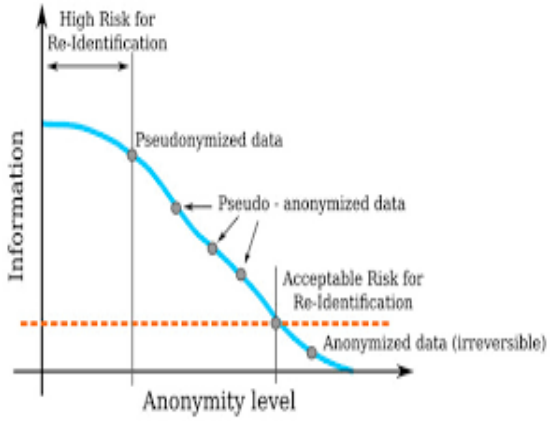


**Figure 8: Calculating Anonymity Level**

## IX. CONCLUSION

Today, all large organisations are required to store a vast amount of data and keep it secure. To prevent unauthorised access to data, we employ a number of cloud computing services. For the purposes of this investigation, only de-identified material will be used. A novel method was proposed for generating pseudonyms so as to ensure that third-party users cannot gain access to the information and also to improve security.

## X. REFERENCES

[1] N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany, and A. Elchouemi, "Enhanced E-health framework for security and privacy in healthcare system," in Proc. 6th Int.

[2] J. Camenisch and A. Lehmann, "(Un)linkable pseudonyms for government databases," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS), 2015, pages 1467–1479.

[3] J. Xu, G. Yang, Z. Chen, and Q. Wang, "A survey on privacy-preserving data aggregation in wireless sensor networks," China Commun., May 2015, vol. 12, no. 5, pp. 162–180.

[4] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy-preserving medical data sharing in the cloud environment," Future Gener.

[5] S. Sharma and D. Shukla, "Efficient multi-party privacy-preserving data mining for vertically partitioned data," in Proc. Int. Conf. Inventive Comput.

[6] M. M. Potey, C. A. Dhote, and D. H. Sharma, "Homomorphic encryption for cloud data security," Procedia Comput. Sci., vol. 79, March 2016, pp. 175–181.

[7] V. Akila and T. Sheela, "Preserving data and key privacy in data aggregation for wireless sensor networks," in Proc. 2nd Int'l Conf. Comput.

[8] K. Gu, N. Wu, B. Yin, and W. J. Jia, to be published in IEEE Trans. Netw. Service Manage., "Secure data query framework for cloud and fog computing"

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12, Dec 2022

[9] Z. Liu, L. Zhang, W. Ni, and I. Collings, to be published in IEEE Trans. Mobile Comput., "Uncoordinated pseudonym changes for privacy preserving in distributed networks."

[10] C. N. H. Vinh, A. Truong, and T. T. Huu, "A privacy-preserving authentication scheme in the intelligent transportation systems," in Proc. Int. Conf. Future Data Secur. Eng.

[11] K.-S. Wu, J.-C. Lee, T.-M. Lo, K.-C. Chang, and C.-P. Chang, ‘‘A secure palm vein recognition system,’’ J. Syst. Softw., vol. 86, no. 11, pp. 2870–2876, Nov. 2013.

[12] S. D. Raut and V. T. Humbe, ‘‘Review of biometrics: Palm vein recognition system,’’ IBMRDs J. Manage. Res., vol. 3, no. 1, pp. 217–223, 2014.

[13] J. A. Unar, W. C. Seng, and A. Abbasi, ‘‘A review of biometric technol- ogy along with trends and prospects,’’ Pattern Recognit., vol. 47, no. 8, pp. 2673–2688, Aug. 2014.

[14] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, ‘‘Toward efficient and privacy-preserving computing in big data era,’’ IEEE Netw., vol. 28, no. 4, pp. 46–50, Jul. 2014.

[15] Terlapu, P. V., Gedela, S. B., Gangu, V. K., & Pemula, R. (2022). Intelligent diagnosis system of hepatitis C virus: A probabilistic neural network based approach. International Journal of Imaging Systems and Technology, 32(6), 2107-2136.

[16] Balasankar, V., Penumatsa, S. V., & Terlapu, P. R. V. (2020). Intelligent socio-economic status prediction system using machine learning models on Rajahmundry AP, SES dataset. Indian Journal of Science and Technology, 13(37), 3820-3842.

[17] Anusha, K. B., Vital, T. P. R., & Sangeeta, K. (2019). Machine Learning Models and Neural Network Techniques for Predicting Uddanam CKD. International Journal of Recent Technology and Engineering (IJRTE), 8(2).

[18]Vital, T. P., Raju, G. P., Sreeramamurthy, K., & Charan, V. V. (2015). A probabilistic neural network approach for classification of datasets collected from north coastal districts of AP, India using MatLab. Procedia Computer Science, 48, 715-721.

[19] Vital, T. P., Nagesh, M. Y. V., Anuradha, T., & Samanthula, A. R. (2016). A neural network approach for classification of kidney disease dataset collected from Visakhapatnam of AP, India. *Int J Innovative Res Sci Eng*, *2*(2).