# DATA ANONYMIZATION USING

# PSEUDONYM SYSTEM TO

# PRESERVE DATA PRIVACY

Sushmitha G M #1 and Prof. Shankar B S\*2

*# PG Scholar, Dept. of MCA, Vidya Vikas Institute Of Engineering and Technology, Mysore,Karnataka, India*

*\*Assistant Professor, Dept. of MCA, , Vidya Vikas Institute Of Engineering and Technology, Mysore,Karnataka, India*

**Abstract**-Organizations routinely collect and store vast amounts of data, leveraging cloud computing and wireless networks for efficiency. These services enable customers to complete tasks swiftly and effectively. Unique identifiers are utilized to catalog data within digital databases, linking sensitive information such as names, addresses, and identification numbers to data owners. However, these identifiers pose potential vulnerabilities; attackers may manipulate them to access entire datasets or engage in eavesdropping to infer necessary details. Consequently, this raises significant concerns regarding data privacy.

The risk of unauthorized access during data transfer is substantial, with potential threats including spoofing and forgery attacks. To address these challenges, this study proposes a biometric authentication approach utilizing palm vein recognition. Additionally, a pseudonymization strategy is employed to anonymize database entries, thereby enhancing data security.

**Index Terms - Canny Edge detector, Pseudonyms Creation technology.**

# I.INTRODUCTION

Utilizing widely accepted techniques may present challenges regarding controllability, as information flow occurs without oversight from a central authority. Their approach facilitates data exchange and management while ensuring user privacy. Findings indicate that the proposed system has been validated through the universal composability (UC) framework,

Findings indicate that the proposed system has been validated through the universal composability (UC) framework, supported by robust examples related to discrete logarithms.

They encourage future researchers to thoroughly investigate the various methodologies documented in the literature for providing secure pseudonyms.

In [3], a study focused on privacy-preserving data aggregation specifically within wireless sensor networks. Various data protection aggregation methods currently in use were categorized and compared based on common privacy preservation techniques. Results revealed that most methods involve an "initialization" phase, where participants establish a secure channel to obtain primary authentication from key issuers. Therefore, developing efficient protocols that operate independently of trusted authorities and maintain secure bidirectional communication channels is essential.

# II. LITERATURE REVIEW

This research presents an innovative anonymization model for Online Social Networks (OSNs), aimed at minimizing the loss of sensitive structural information while achieving a high level of anonymity. We introduce an effective clustering-based anonymization method for privacy-preserving data collection in IoT-enabled healthcare services. The healthcare sector has undergone significant changes due to the rapid advancement of the Internet of Things. Our proposed scheme focuses on maintaining privacy during data collection in IoT healthcare systems. Additionally, we offer a zero-delay anonymization framework for data streams, which translates z-anonymity into the k-anonymity property. Our findings suggest that careful selection of z-anonymity parameters enables data curators to likely generate k-anonymized datasets with a quantifiable probability. Lastly, we address critical factors related to privacy protection on social networking sites. This study aims to explore the factors influencing information privacy concerns and protective behaviors associated with the use of social networking sites. The factors are derived from protection motivation theory, hyperpersonal communication framework, and privacy protection behaviors. The rapid expansion of social networking platforms has encouraged active participation from diverse users, resulting in heightened security and privacy concerns. To address these issues, this paper presents a secure and privacy-preserving strategy for safeguarding user data across cloud-based online social networks.

III. PROPOSED WORK

The primary goal of this research is to utilize palm vein patterns to ensure data privacy through the pseudonymization technique. As previously noted, palm vein patterns are a reliable biometric characteristic suitable for pseudonym generation.

The pseudonyms are created using a homomorphic encryption approach, highlighting the proposed privacy protection strategy. For this study, palm vein images were captured using a palm vein scanner. The acquired images often require filtering to eliminate noise. Edge detection is employed to analyze the feature boundaries. Several key points within the selected features are considered to effectively transform intravascular signals into a secret key.

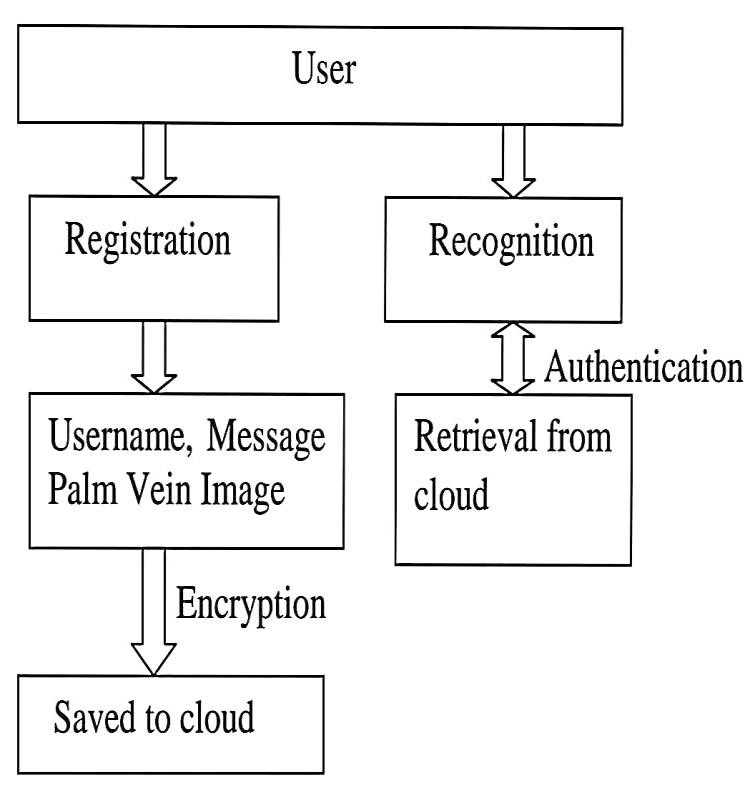
Two partial keys are derived from the palm vein patterns to demonstrate that the proposed method can safeguard online privacy against potential attacks. Finally, the complete alias is constructed using the available keys

# IV ADVANTAGES

**Advantage:**  
The system identifies palm vein patterns as a reliable biometric feature for generating pseudonyms. These pseudonyms are created using a homomorphic encryption method, highlighting the suggested privacy protection strategy. For this study, palm vein images were captured using a palm vein scanner.The collected images often require filtering to remove noise. Edge detection is employed to analyze the feature boundaries. Several key points within the selected features are considered to effectively convert intravascular signals into a secret key. Two partial keys are derived from the palm vein patterns to demonstrate that the proposed

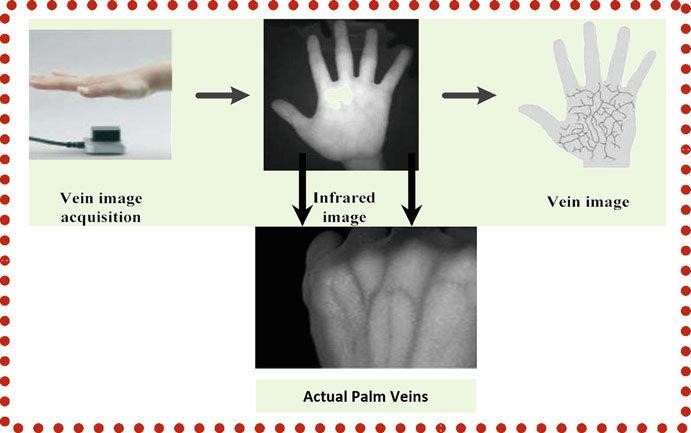
method can safeguard online privacy against potential attacks. features considered to effectively transform intravascular signals into a secret key. Two partial keys are generated from the palm vein patterns to demonstrate that the proposed method can protect online privacy against anticipated attack attempts. Subsequently, the final alias is constructed using the generated keys.

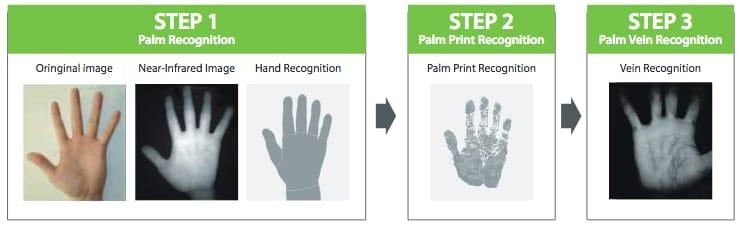
# V. SYSTEM ARCHITECTURE

System architecture is depicted through a diagram that presents the comprehensive structure of a software system, highlighting the relationships and boundaries between its components. This diagram is a critical tool, as it provides a holistic view of the system, facilitating a thorough understanding of the interaction and functionality of its various parts. In the realm of Data Anonymization Using Pseudonyms, the system architecture diagram plays a vital role in safeguarding data privacy. It aids in pinpointing and managing the components involved in data anonymization, ensuring that sensitive information is effectively protected.

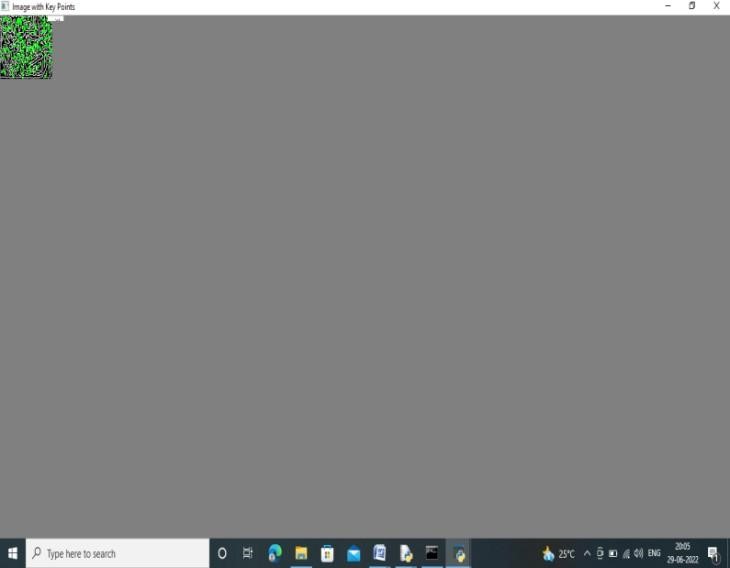
The architecture focuses on utilizing a pseudonym creation technique to generate pseudonyms that protect individual identities and their sensitive information. This process involves using palm vein images, and to extract feature key points, the Canny Edge Detector algorithm is employed in this project development.

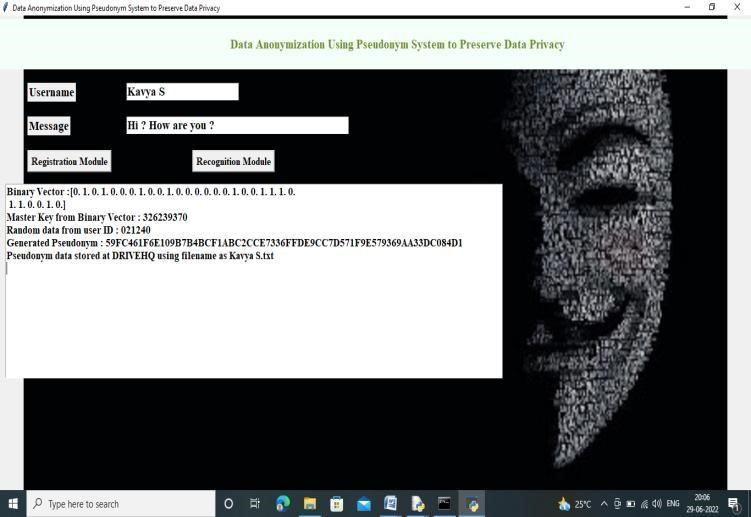
VI. EXPIRIMENTAL RESULT

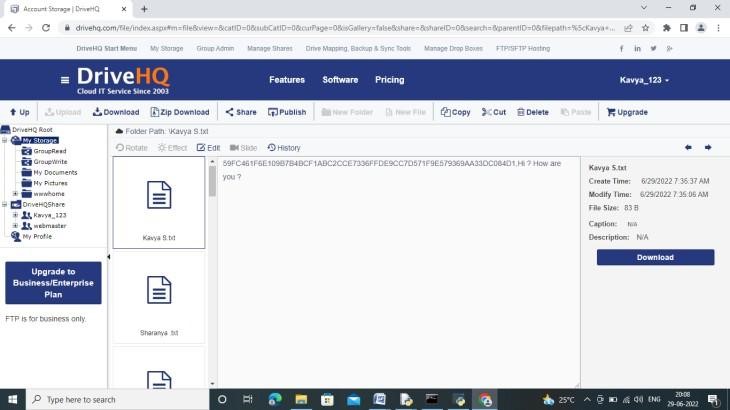




Initially, obtaining Palm Vein images from the Palm Vein database is crucial. To recognize the Palm Vein pattern, smoothing the Palm Vein using a Gaussian filter is essential to remove noise. Applying a Median Filter is then necessary to eliminate white and black dots. This process helps in detecting feature key points, which are used to generate binary vectors. These binary vectors contribute to generating a master key, which in turn aids in creating pseudonyms to safeguard sensitive information.







# VII CONCLUSION

In today's landscape, businesses and organizations are mandated to store and protect vast volumes of data efficiently. The efficient handling of such data often involves the utilization of cloud computing services. Given the imperative of data protection, the focus of this inquiry is on anonymized data. A novel approach has been developed for the creation of pseudonyms that ensures the maintenance of confidentiality.

# VIII 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. Conf. Digit. Inf. Process. Commun. (ICDIPC), Apr. 2016, pp. 75–79.
2. J. Camenisch and A. Lehmann, ‘‘(Un)linkable pseudonyms for governmental databases,’’ in Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2015, pp. 1467–1479.
3. J. Xu, G. Yang, Z. Chen, and Q. Wang, ‘‘A survey on the privacypreserving data aggregation in wireless sensor networks,’’ China Commun., vol. 12, no. 5, pp. 162–180, May 2015.
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. Comput. Syst., vols. 43–44, pp. 74–86, Feb. 2015.
5. M. M. Potey, C. A. Dhote, and D. H. Sharma,

‘‘Homomorphic encryption for security of cloud data,’’ Procedia Comput. Sci., vol. 79, pp. 175–181, Mar. 2016.