

PRIVACY PRESERVATION SCHEME OF FACE IDENTIFICATION WITH MULTIPARTY ACCESS IN NET BANKING ENVIRONMENTS USING IOT

A . Rabik,
Student,

Department of Computer Science and Engineering,
Sudharsan Engineering College,
Pudukkottai, Tamilnadu, India.

A.Arun Pandi,
Student,

Department of Computer Science and Engineering,
Sudharsan Engineering College,
Pudukkottai, Tamilnadu, India.

S.Ajith Kumar,
Student,

Department of Computer Science and Engineering,
Sudharsan Engineering College,
Pudukkottai, Tamilnadu, India.

P. Arockia Mary,
Associate Professor,

Department of Computer Science and Engineering,
Sudharsan Engineering College,
Pudukkottai, Tamilnadu, India.

Abstract: Identification can be equated to a username and is used to authorize access to a system. Implement Face biometric systems with iterative closest point algorithm and K-NN classification algorithm. And also allow sub-users to access our accounts based on our permission with SMS alerts. Implement Face biometric systems to authorize the person at the time of money transfer or account maintenance. Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification and resolution raises the demands of computation.

Keywords: *Internets of Things (IoT), face identification, face resolution, security, privacy preservation.*

I. INTRODUCTION

The Internets of Things (IoT) realizes the interconnection and intercommunication among ubiquitous things, and promotes the natural and seamless convergence of physical space and cyber space. More and more physical objects, including humans, sensors, mobile devices, are connected into Internet to be an element of IoT in various application. As a special physical object, humans are also frequently interacting with cyber space. Currently, Internet Of People (IoP) based applications are attracting even more attention. The Internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

In the Internet of Things (IoT), identification and resolution of physical object is crucial for authenticating object's identity, controlling service access, and establishing trust between object and cloud service. With the development of computer vision and pattern recognition technologies, face has been used as a high-security identification and identity authentication method which has been deployed in various applications.

Face identification can ensure the consistency between individual in physical-space and his/her identity in cyber-space during the physical-cyber space mapping. However, face is a non-code and unstructured identifier. With the increase of applications in current big data environment, the characteristic of face identification will result in the growing demands for

computation power and storage capacity. In this paper, we propose a face identification and resolution scheme based on cloud computing to solve the above problem. The face identification and resolution system model is presented to introduce the processes of face identifier generation and matching. Then, parallel matching mechanism and cloud computing-based resolution framework are proposed to efficiently resolve face image, control personal data access and acquire individual's identity information. It makes full use of the advantages of cloud computing to effectively improve computation power and storage capacity. The experimental result of prototype system indicates that the proposed scheme is practically feasible and can provide efficient face identification and resolution service.

The identification and resolution technology are the prerequisite for realizing identity consistency of physical-cyber space mapping in the Internet of Things (IoT). Face, as a distinctive noncoded and unstructured identifier, has especial advantages in identification applications. With the increase of face identification based applications, the requirements for computation, communication, and storage capability are becoming higher and higher. To solve this problem, we propose a fog computing based face identification and resolution scheme. Face identifier is first generated by the identification system model to identify an individual. Then, a fog computing based resolution framework is proposed to efficiently resolve the individual's identity. Some computing overhead is offloaded from a cloud to network edge devices in order to improve processing efficiency and reduce network transmission. Finally, a prototype system based on Local Binary Patterns (LBP) identifier is implemented to evaluate the

scheme. Experimental results show that this scheme can effectively save bandwidth and improve efficiency of face identification and resolution.

II. RELATED WORK

Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification and resolution raises the demands of computation communication and storage capabilities. Therefore, we have proposed the fog computing based face identification and resolution framework to improve processing capacity and save the bandwidth. However, there are some security and privacy issues brought by the properties of fog computing based framework. In this paper, we propose a security and privacy preservation scheme to solve above issues. We give an outline of the fog computing based face identification and resolution framework, and summarize the security and privacy issues. Then the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are proposed to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution. Finally, we implement a prototype system to evaluate the influence of security scheme on system performance. Meanwhile, we also evaluate and analyze the security properties of proposed scheme from the viewpoint of logical formal proof and the CIA (confidentiality, integrity, availability) properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation [1].

In this paper, we propose a novel face recognition approach based on 2.5D/3D shape matching. While most of existing methods use facial intensity image, we aim to develop a method using three-dimensional information of the human face. This is the main innovation of our technology. In our approach, the 3D dimensional information is introduced in order to overcome classical face recognition problems which are pose, illumination and facial expression variations. The paradigm is to build a 3D face gallery using a laser-based scanner: the off-line stage. In the on-line stage, the recognition, we capture one 2.5D face model at any view point and with any facial expressions. Our processing allows the identification of the presented person by performing the captured model with all faces from the database. Here, the Iterative Closest Point-based matching algorithm provides the pose of the probe whereas the region-based metric provides a spatial deviation between the probe and each face from the gallery. In this metric, we calculate the global recognition score as a weighted sum of region-based distances already labelled as mimic or static regions. For automatic 3D face segmentation, we use an immersion version of watershed segmentation algorithm. This paper also presents some experiments in order to show illumination, pose and facial expression compensations [2].

In this section, we describe the face identifier generation model and fog computing based face identification system. The face identification system plays a significant role in efficient representing and identifying an individual's identity, and it is closely related to face resolution. A good identification model is not only helpful to the face classification and resolution, but also can reduce the amount of data stored in the database. The identification and resolution technology are the prerequisite for

realizing identity consistency of physical-cyber space mapping in the Internet of Things (IoT). Face, as a distinctive non coded and unstructured identifier, has especial advantages in identification applications. With the increase of face identification based applications, the requirements for computation, communication, and storage capability are becoming higher and higher. To solve this problem, we propose a fog computing based face identification and resolution scheme. Face identifier is first generated by the identification system model to identify an individual. Then, a fog computing based resolution framework is proposed to efficiently resolve the individual's identity. Some computing overhead is offloaded from a cloud to network edge devices in order to improve processing efficiency and reduce network transmission. Finally, a prototype system based on local binary patterns (LBP) identifier is implemented to evaluate the scheme. Experimental results show that this scheme can effectively save bandwidth and improve efficiency of face identification and resolution [3].

III. SYSTEM MODEL

Implement real time authentication system using face biometrics for authorized the person for online banking system. And also provide multiparty access system to allow the multiple persons to access the same accounts by providing access privileges to original account holders. Overcome the guessing attacks and dictionary attacks. Without primary user knowledge, no one perform fraud activities. No need to implement additional sensors. SMS alert to know about transactions details up to date. Multi-party access with improved security.

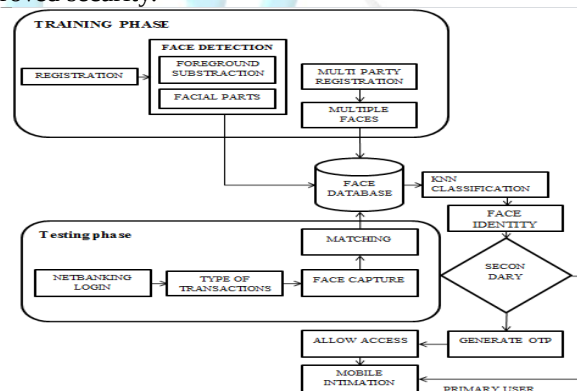
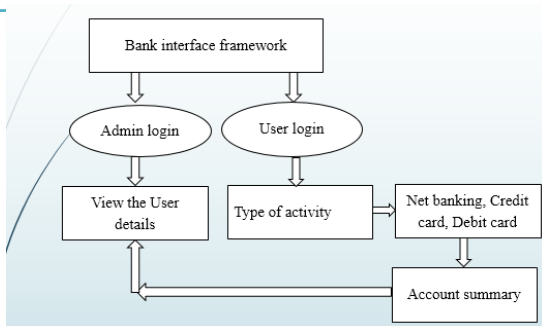


Figure 1: Proposed System Architecture

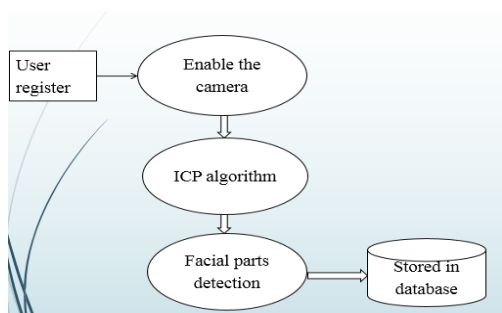
A. Bank interface creation

Online banking is thus changing the way people shop and how retailers operate. In this module, admin and user interface created. Admin can be view the details of users, accounts details and so on. The user can be performing various operations such as net banking, credit card transaction, debit card transactions and on.



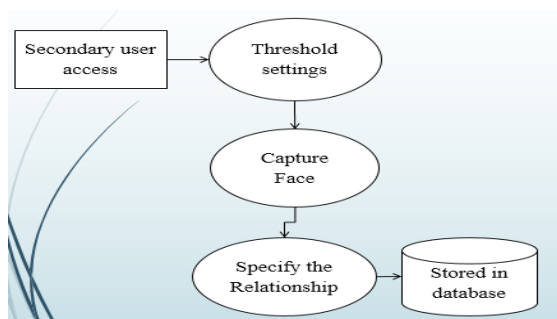
B . Face detection

In this module, we can implement features based method to detect the facial parts such as nose, lips, eyes, cheeks using Iterative Closest Point(ICP) algorithm. We use, for performing ICP, a set of features selected based on the tolerance level of spatial deviation.



B. Access permissions

Multi-party authorization (MPA) is a process to protect online transactions from undesirable acts by a malicious insider or inexperienced technician acting alone. In this module, user of account specified as primary user. In this module, primary user provides access permission to secondary users with predefined threshold values. Admin can store details of secondary users with relationship information.



C. Face verification

In this module, perform the verification of multiple users using classification algorithm named as K-Nearest Neighbor Classification. The k-nearest neighbor algorithm (k-NN) is a method for classifying objects based on closest training examples in the feature space.

E .OTP generation

One time password can be generated using SHA-3 algorithm. Hash algorithms are fundamental to many cryptographic

applications. Although widely associated with digital signature technology, the hash algorithm has a range of other uses. A secure hash algorithm, often known simply as an “SHA,” is a hashing algorithm that is considered cryptographically secure.

F .SMS notification

Finally provide SMS alert to primary users about the transactions. The details of the transactions has user name of account access, timing details, amount details, mode of payments and so on. Based on these details, primary user easily know the transactions details up to date.

IV. EXPERIMENTAL RESULTS

The following figure illustrates the bank interface creation window of the proposed system .

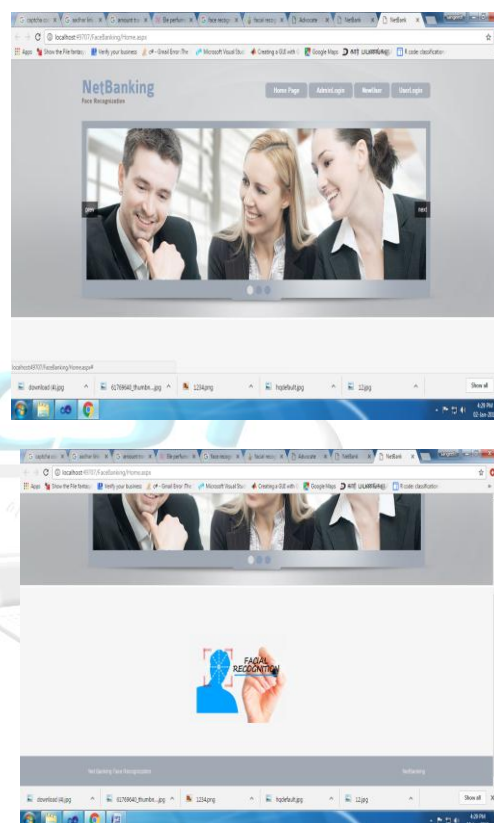


Figure 2: Bank interface creation window

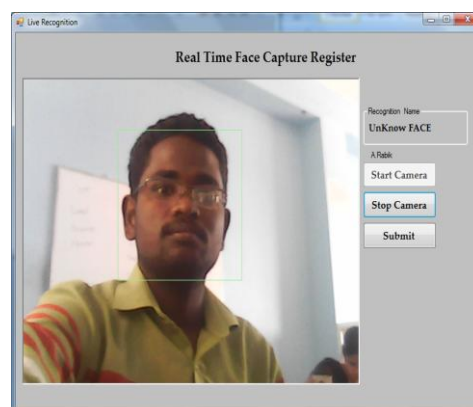


Figure 3: Face Detection window

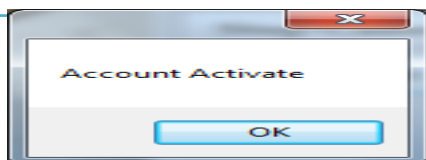


Figure4:Account Activate Window

IV Algorithm: ICP-based matching

Inputs: $P = \{p_i\}$ (model from database), $X = \{y_i\}$ (scan model)

Outputs: (R, T) which minimize MSE, matched points, spatial deviation

- Find closest point pairs (init.: coarse alignment solution)
- Compute best transform which minimizes the MSE,
- Apply transform to the scan model,
- Iterate until numerical convergence, compute at each iteration (R_k, T_k) ,



Figure 5. Iterative Closest Point for fine alignment

V.KNN CLASSIFICATION

As discussed earlier, we consider each of the characteristics in our training set as a different dimension in some space, and take the value an observation has for this characteristic to be its coordinate in that dimension, so getting a set of points in space. We can then consider the similarity of two points to be the distance between them in this space under some appropriate metric.

Input: D , the set of k training objects, and test object $z=(x', y')$

Process:

Compute $d(x', x)$, the distance between z and every object $(x, y) \in D$.

Select $D_z \leq D$, the set of k closest training objects to z .

Output : $y' = \arg\max_{(x, y) \in D_z} I(u=y_i)$

VI. CONCLUSIONS

The security and privacy-preservation schemes for face identification and face resolution have been proposed. Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based security systems. To accurately and thoroughly accomplish this demands a high level of user involvement.

VII. REFERENCES

- [1]. Pengfei Hu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Tie Qiu, Senior Member, IEEE, Houbing Song, Senior Member, IEEE, Yanna Wang, and Xuanxia Yao "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things" IEEE INTERNET OF THINGS JOURNAL VOL: 4, NO: 5, OCT. 2017.
- [2]. Boulbaba Ben Amor¹, Karima Ouji¹, Mohsen Ardabilian¹, Liming Chen¹ LIRIS Lab, Lyon Research Center for Images and Intelligent Information Systems, UMR 5205 CNRS Centrale Lyon, France "3D Face recognition by ICP-based shape matching"
- [3]. N. N. Khan, "Fog Computing: A Better Solution For IoT," International Journal of Engineering and Technical Research, vol. 3, no. 2, pp. 298- 300, 2015.
- [4]. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, 2012, pp. 13-16.
- [5]. P. Hu, H. Ning, T. Qiu, Y. Zhang, X. Luo, "Fog Computing-Based Face Identification and Resolution Scheme in Internet of Things," IEEE Transactions on Industrial Informatics, 2016. [Online]. Available: <https://doi.org/10.1109/TII.2016.2607178>
- [6]. T. Qiu, A. Zhao, R. Ma, V. Chang, F. Liu, and Z. Fu, "A task efficient sink node based on embedded multi-core SoC for Internet of Things," Future Generation Computer Systems, 2016. [Online]. Available: <http://dx.doi.org/10.1016/j.future.2016.12.024>
- [7]. Y. Zheng, Z. Peng, and A. V. Vasilakos, "A Survey on Trust Management for Internet of Things," Journal of Network and Computer Applications, vol. 42, no. 3, pp. 120-134, 2014.
- [8]. H. Song, G. A. Fink, and S. Jeschke, Security and Privacy in Cyber- Physical Systems: Foundations, Principles and Applications. Chichester, UK: Wiley-IEEE Press, 2017.