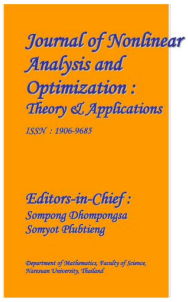
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



COGNIZANT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION

Kaluvala Swapna , Assistant Professor CSE , Vaagdevi College of Engineering(Autonomous) , India
Kolanu Pavani , UG Student , CSE , Vaagdevi College of Engineering (Autonomous) , India
Madde Divya , UG Student , CSE , Vaagdevi College of Engineering (Autonomous) , India
Mohammed Ayaanuddin , UG Student , CSE , Vaagdevi College of Engineering (Autonomous) , India
Manchala Nithin , UG Student , CSE , Vaagdevi College of Engineering (Autonomous) , India

ABSTRACT

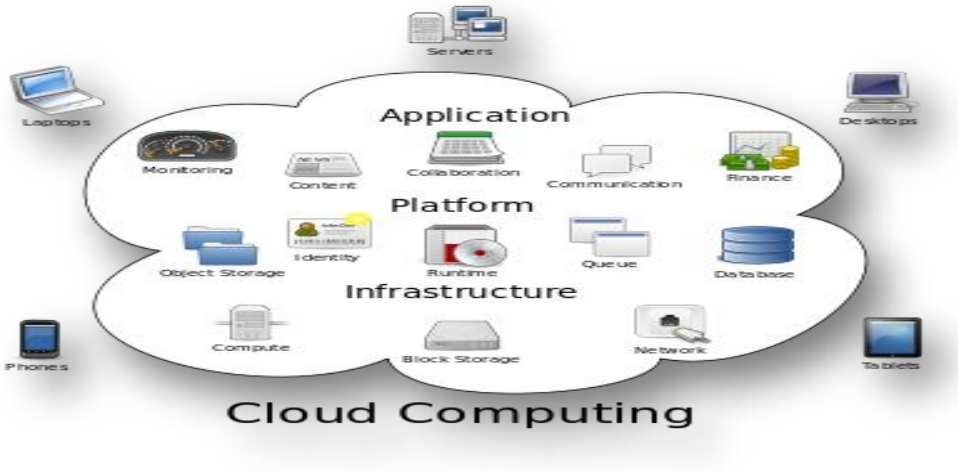
Biometric identification has become increasingly popular in recent years. With the developmentof cloud computing, database owners are motivated to outsource the large size of biometric data andidentification tasks to the cloud to get rid of the expensive storage and computation costs, which howeverbrings potential threats to users' privacy. In this paper, we propose an efficient and privacy-preservingbiometric identification outsourcing scheme. Specifically, the biometric data is encrypted and outsourcedto the cloud server. To execute a biometric identification, the database owner encrypts the query data andsubmits it to the cloud. The cloud performs identification operations over the encrypted database and returnsthe result to the database owner. A thorough security analysis indicates the proposed scheme is secure evenif attackers can forge identification requests and collude with the cloud. Compared with previous protocols,experimental results show the proposed scheme achieves a better performance in both preparation andidentification procedures.

Index : biometric, identification, identification task , privacy, security, efficient, security analysis

1. INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

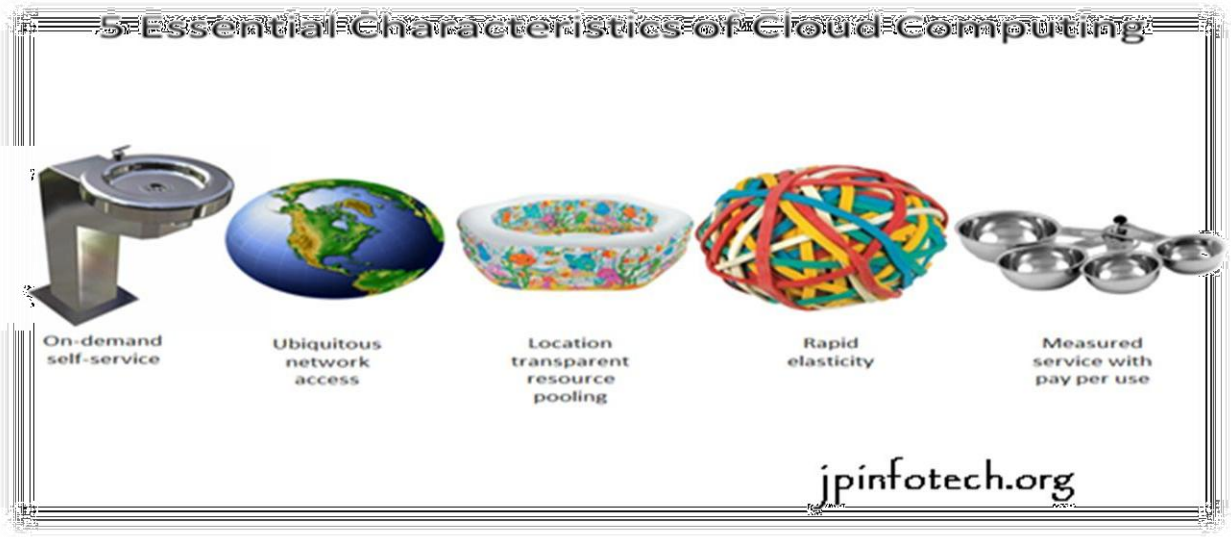
The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

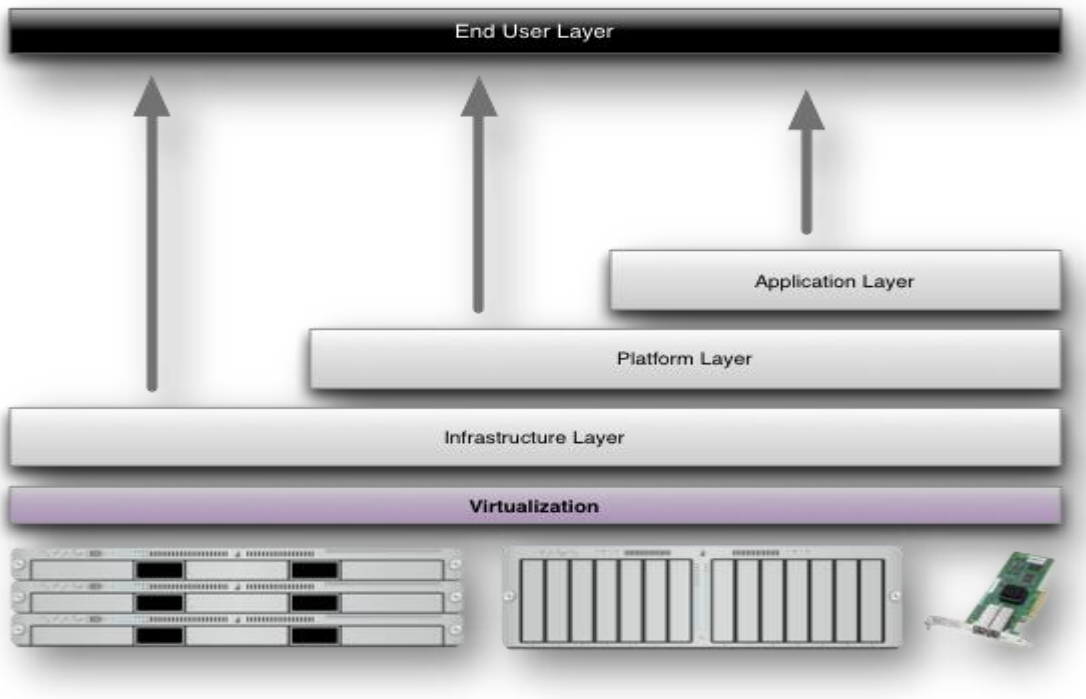
- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.



Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.



Structure of service models

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.

10. **Improve flexibility.** You can change direction without serious “people” or “financial” issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud’s core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

2. LITERATURE SURVEY

1) PRIVACY-PRESERVING FINGERCODE AUTHENTICATION.

AUTHORS: Mauro Barni, Mario Di Raimondo, Tiziano Bianchi, and Dario Catalano

We present a privacy preserving protocol for fingerprintbased authentication. We consider a scenario where a client equipped with a fingerprint reader is interested into learning if the acquired fingerprint belongs to the database of authorized entities managed by a server. For security, it is required that the client does not learn anything on the database and the server should not get any information about the requested biometry and the outcome of the matching process. The proposed protocol follows a multi-party computation approach and makes extensive use of homomorphic encryption as underlying cryptographic primitive. To keep the protocol complexity as low as possible, a particular representation of fingerprint images, named Fingercode, is adopted. Although the previous works on privacy-preserving biometric identification focus on selecting the best matching identity in the database, 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 fingercode is under a given threshold. Variants for simple authentication purposes are provided. Our protocols gain a notable bandwidth saving (about 8 − 24%) if compared with the best previous work [1] and its computational complexity is still low and suitable for practical applications. Moreover, even if such protocols are presented in the context of a fingerprintbased system, they can be generalized to any biometric system that shares the same matching methodology, namely distance computation and thresholding.

2) Efficient privacy-preserving biometric identification

AUTHORS: Yan Huang, Lior Malka, David Evans, and Jonathan Katz

We present an efficient matching protocol that can be used in many privacy-preserving biometric identification systems in the semi-honest setting. Our most general technical contribution is a new backtracking protocol that uses the byproduct of evaluating a garbled circuit to enable efficient oblivious information retrieval. We also present a more efficient protocol for computing the Euclidean distances of vectors, and optimized circuits for finding the closest match between a point held by one party and a set of points held by another. We evaluate our protocols by implementing a practical privacy-preserving fingerprint matching system.

3. Collusion-resisting secure nearest neighbor query over encrypted data in cloud

AUTHORS Youwen Zhu ; Zhikuan Wang ; Jian Wang

It is a challenging problem to securely resist the collusion of cloud server and query users while implementing nearest neighbor query over encrypted data in cloud. Recently, CloudBI-II is put forward to support nearest neighbor query on encrypted cloud data, and declared to be secure while cloud server colludes with some untrusted query users. In this paper, we propose an efficient attack method which indicates CloudBI-II will reveal the difference vectors under the collusion attack. Further, we show that the difference vector disclosure will result in serious privacy breach, and thus attain an efficient attack method to break CloudBI-II. Namely, CloudBI-II cannot achieve their declared security. Through theoretical analysis and experiment evaluation, we confirm our proposed attack approach can fast recover the original data from the encrypted data set in CloudBI-II. Finally, we provide an enhanced scheme which can efficiently resist the collusion attack.

4. Security analysis on privacy-preserving cloud aided biometric identification schemes

Biometric identification (BI) is the task of searching a pre-established biometric database to find a matching record for an enquiring biometric trait sampled from an unknown individual of interest. This has recently been aided with cloud computing, which brings a lot of convenience but simultaneously arouses new privacy concerns. Two cloud aided BI schemes pursuing privacy preserving have recently been proposed by Wang et al. in ESORICS ’15. In this paper, we propose several elaborately designed attacks to reveal the security breaches in these two schemes. Theoretical analysis is given to validate our proposed attacks, which indicates that via such attacks the cloud server can accurately infer the outsourced database and the identification request.

3. PROBLEM STATEMENT

Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which however brings potential threats to users' privacy. In a biometric identification system, the database owner such as the FBI who is responsible to manage the national fingerprints database, may desire to outsource the enormous biometric data to the cloud server (e.g., Amazon) to get rid of the expensive storage and computation costs.

3.1 Problem Identification

The existing system for Cognizant Biometric Recognition with Efficiency and Privacy Protection, despite its groundbreaking approach, suffers from several drawbacks. It often faces challenges in real-time processing due to its complex privacy protection algorithms, leading to occasional delays in identification. Furthermore, its reliance on centralized data storage can make it a potential target for large-scale cyberattacks. There are also concerns regarding its adaptability to diverse biometric input types, with certain modalities not being recognized as efficiently as others. Moreover, the system demands rigorous maintenance and updates to stay ahead of emerging threats, incurring both time and monetary costs.

4. PROPOSED SYSTEM

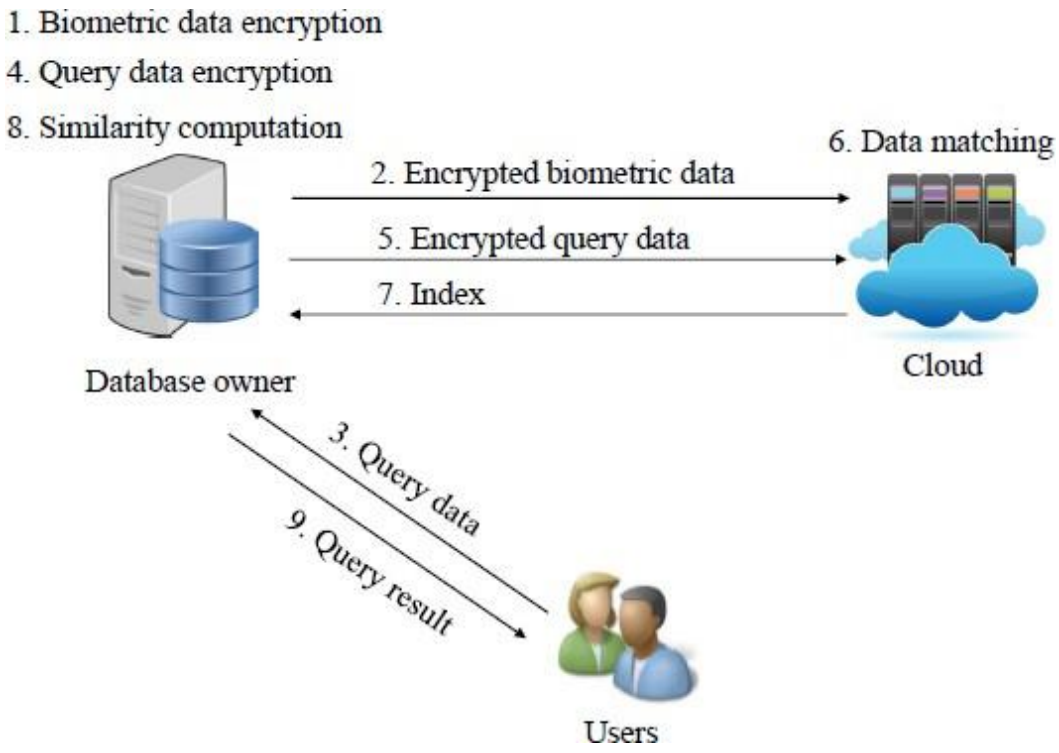
we propose an efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users and the cloud. Specifically, our main contributions can be summarized as follows:

We examine the biometric identification scheme and show its insufficiencies and security weakness under the proposed level-3 attack. Specifically, we demonstrate that the attacker can recover their secret keys by colluding with the cloud, and then decrypt the biometric traits of all users. We present a novel efficient and privacy-preserving biometric identification scheme. The detailed security analysis shows that the proposed scheme can achieve a required level of privacy protection. Specifically, our scheme is secure under the biometric identification outsourcing model and can also resist the attack proposed .Compared with the existing biometric identification schemes, the performance analysis shows that the proposed scheme provides a lower computational cost in both preparation and identification procedures.

4.1 Advantages Of System

To realize the efficiency and secure requirements, we have designed a new encryption algorithm and cloud authentication certification. The detailed analysis shows it can resist the potential attacks.

5. SYSTEM ARCHITECTURE:



6. IMPLEMENTATION

6.1 Database Owner

The database owner holds a large size of biometric data (i.e., fingerprints, irises, voice, and facial patterns etc.), which is encrypted and transmitted to the cloud for storage . After receiving the request, the database owner generates a ciphertext for the biometric trait and then transmits the ciphertext to the cloud for identification. Database owner computes the similarity between the query data and the biometric data associated with the index, and returns the query result to the user.

6.2 Data User:

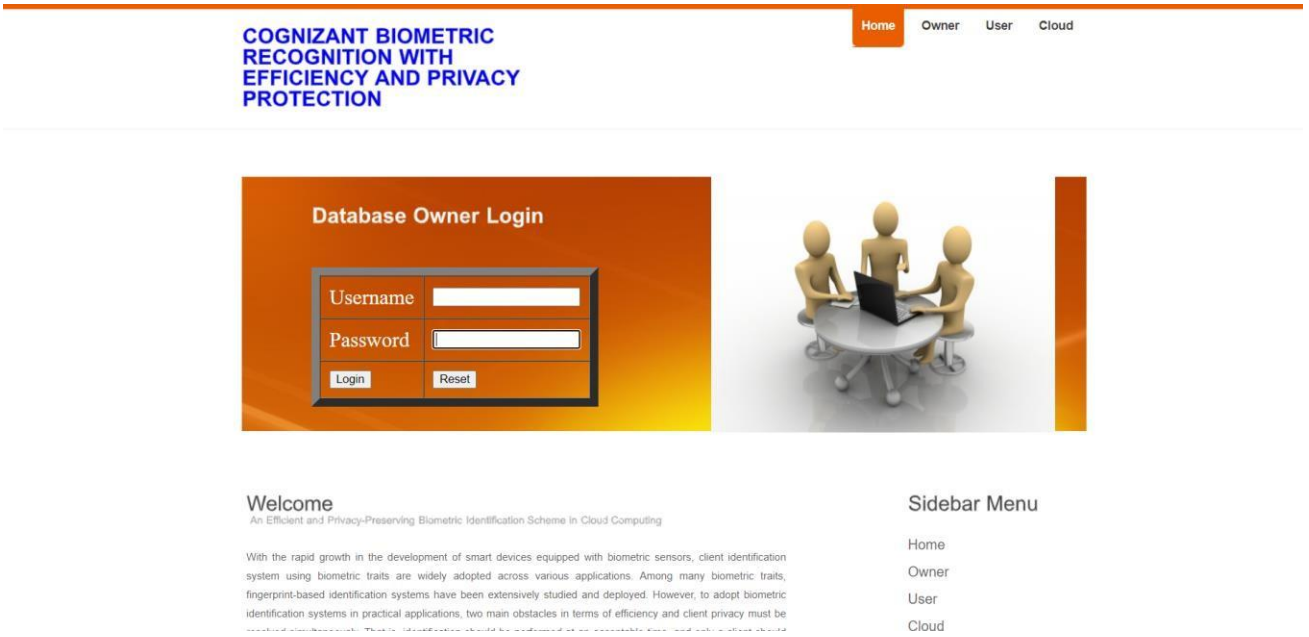
When a user wants to identify himself/herself, a query request is be sent to the database owner.

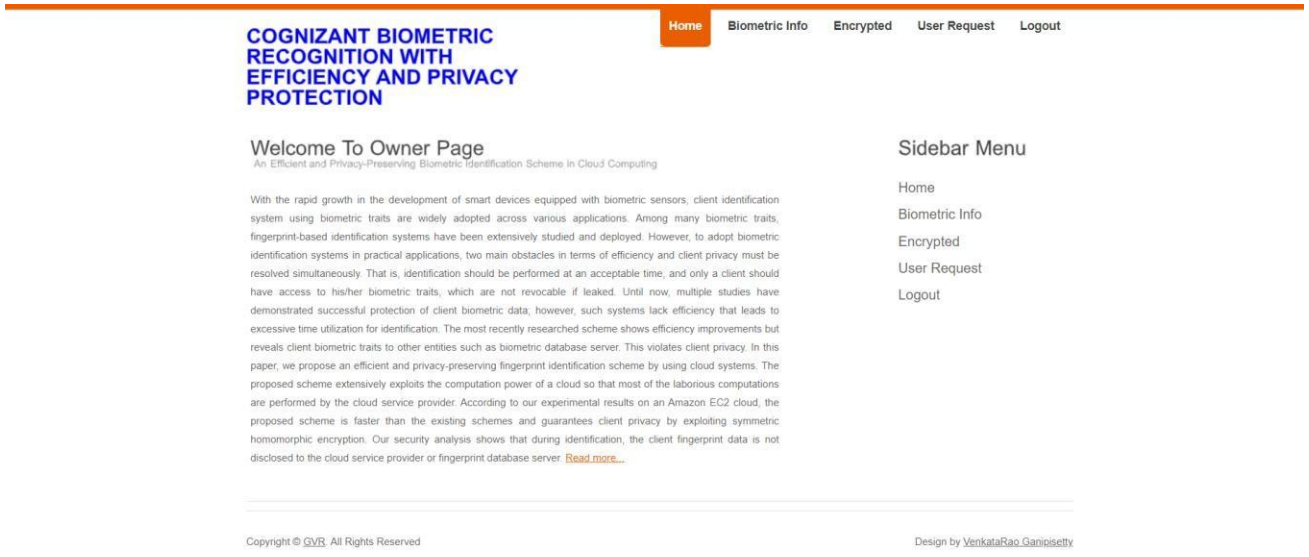
6.3 Cloud Server:

The cloud server figures out the best match for the encrypted query and returns the related index to the database owner.

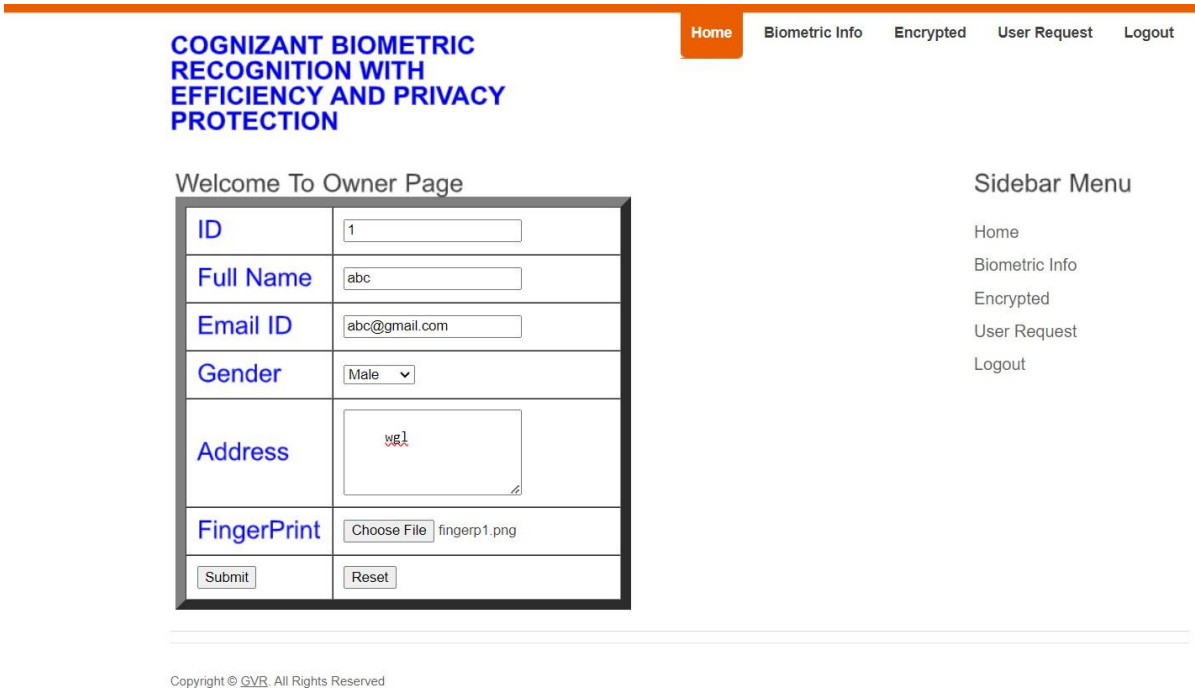
7. SCREENSHOTS

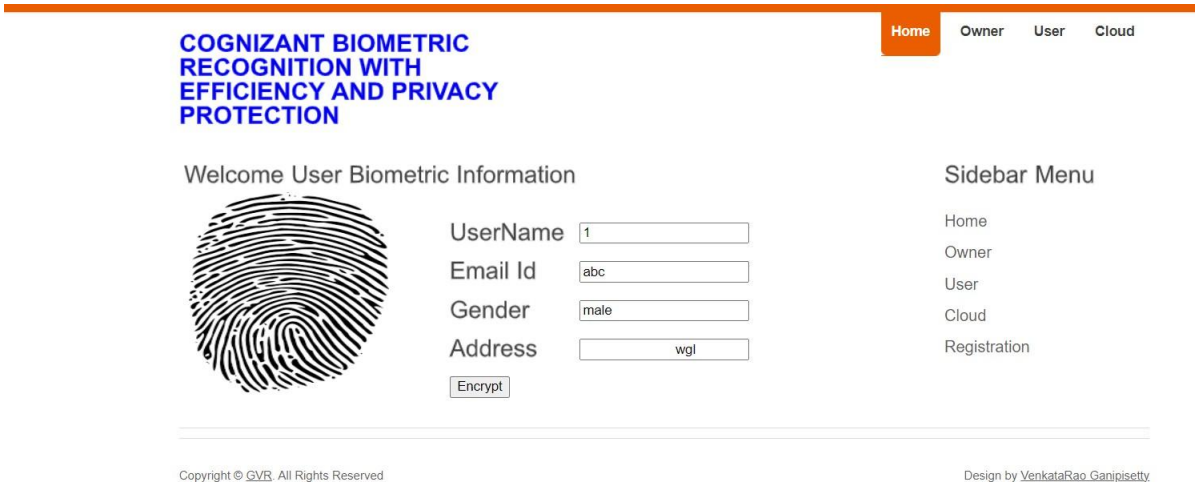
7.1 Homepage



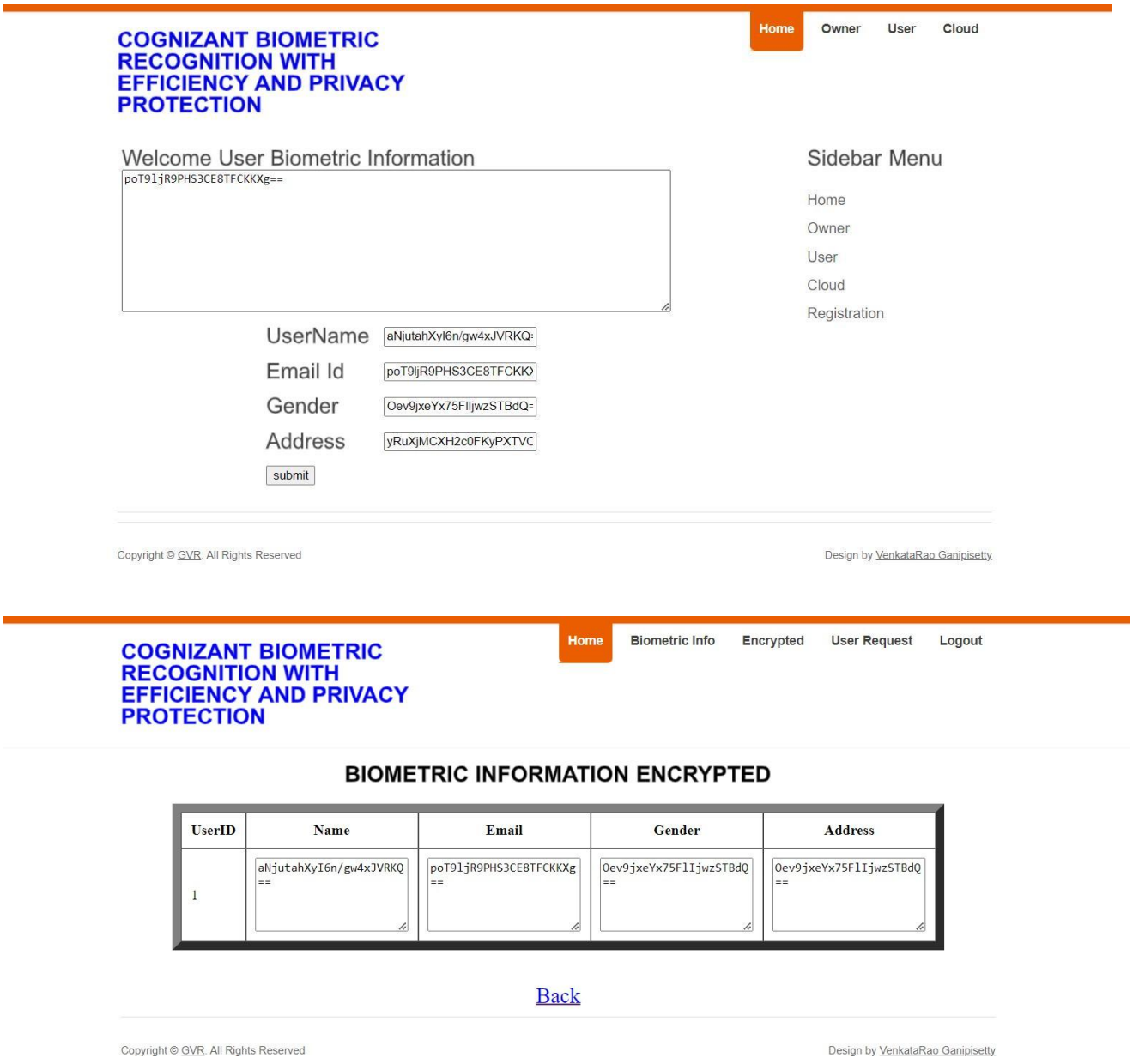


7.2 Database Owner Login

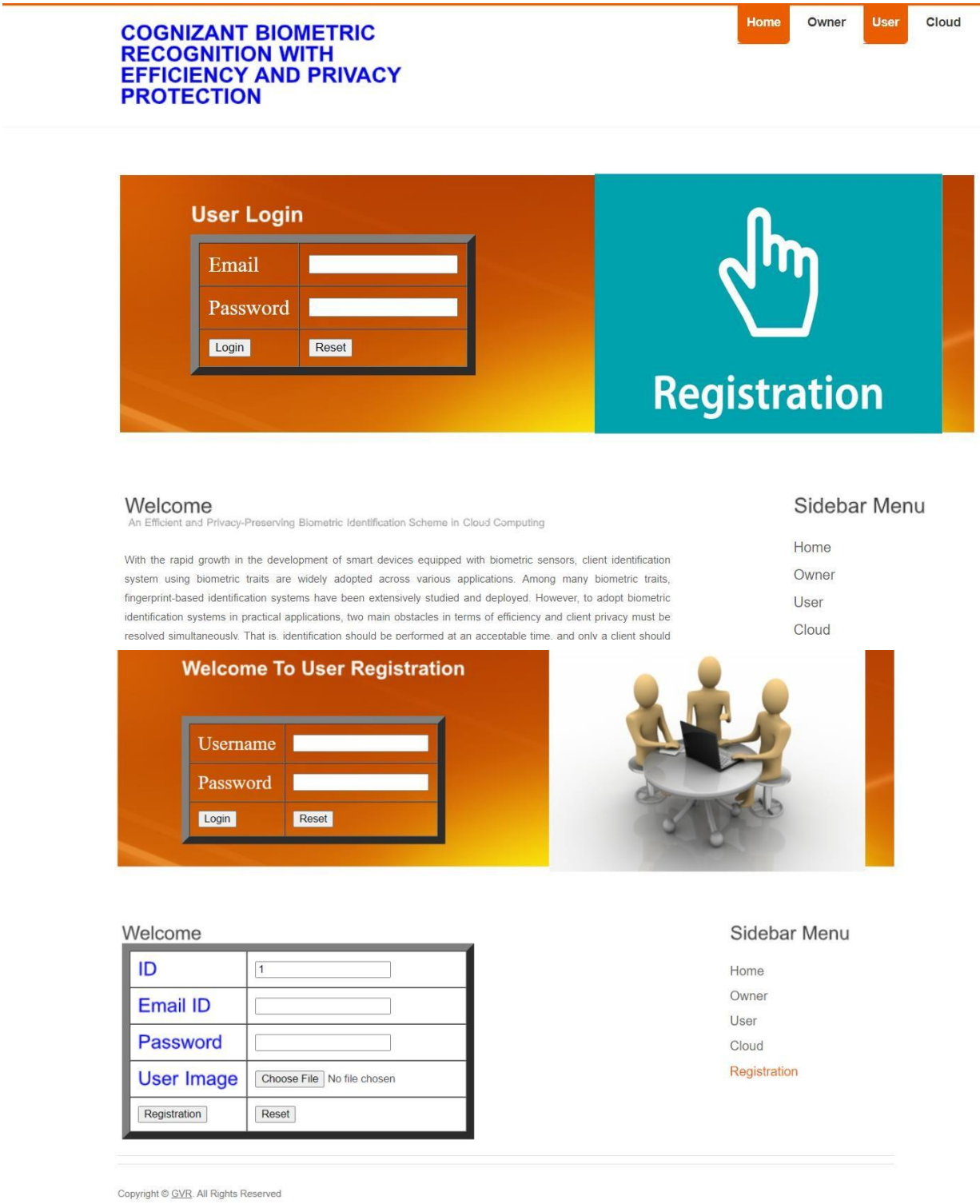




7.3 User Biometric Information



7.4 Biometric Information Encrypted



7.5 User registration

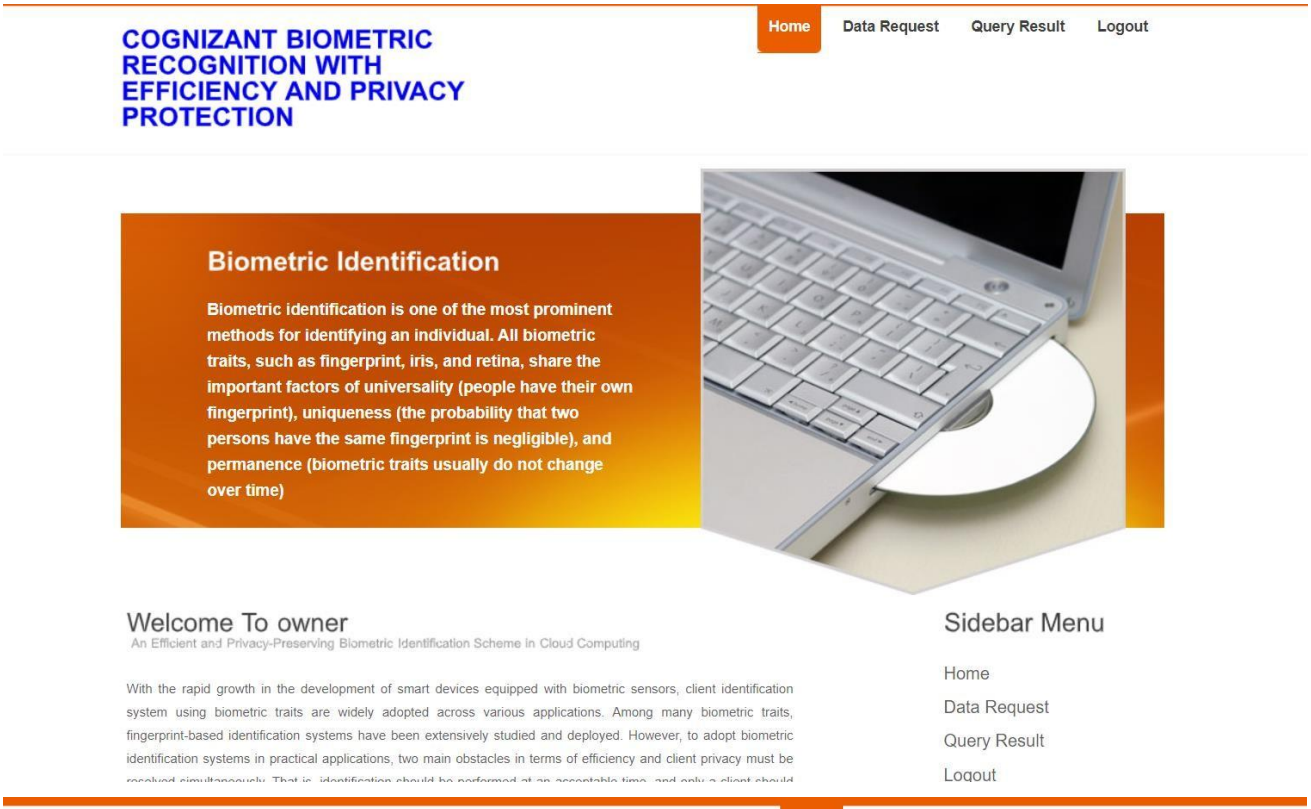

Welcome To User Registration
Username
Password
Login
Reset

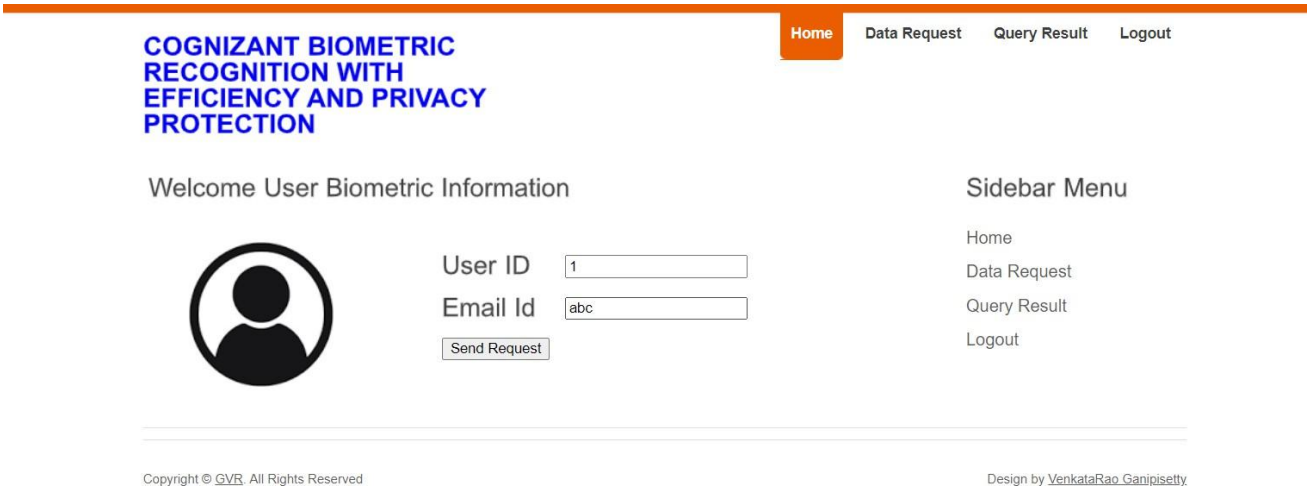

Welcome
ID
1
Email ID
abc@gmail.com
Password
User Image
Choose File
userimage.png
Registration
Reset
Sidebar Menu
Home
Owner
User
Cloud
Registration
Copyright © GVR. All Rights Reserved


COGNIZANT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION
Home
Owner
User
Cloud

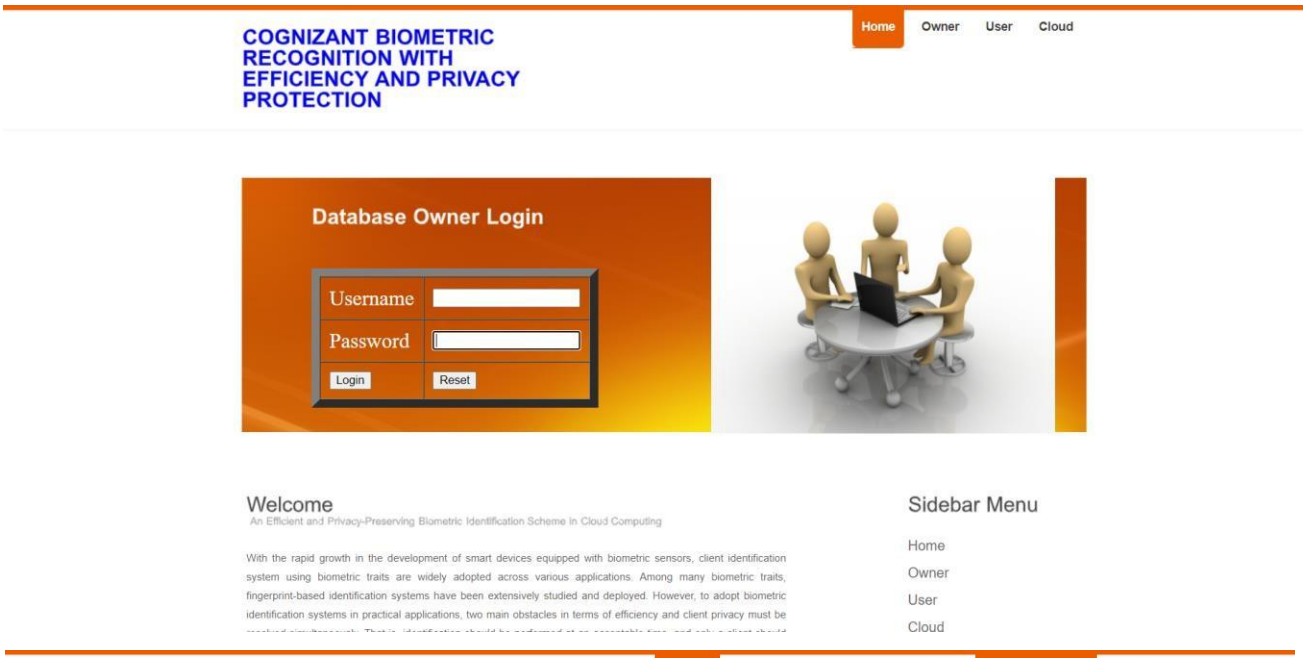

User Login
Registration Completed
Email
abc@gmail.com
Password
Login
Reset
Registration


Welcome
An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing
With the rapid growth in the development of smart devices equipped with biometric sensors, client identification system using biometric traits are widely adopted across various applications. Among many biometric traits, fingerprint-based identification systems have been extensively studied and deployed. However, to adopt biometric identification systems in practical applications, two main obstacles in terms of efficiency and client privacy must be
Sidebar Menu
Home
Owner
User
Cloud

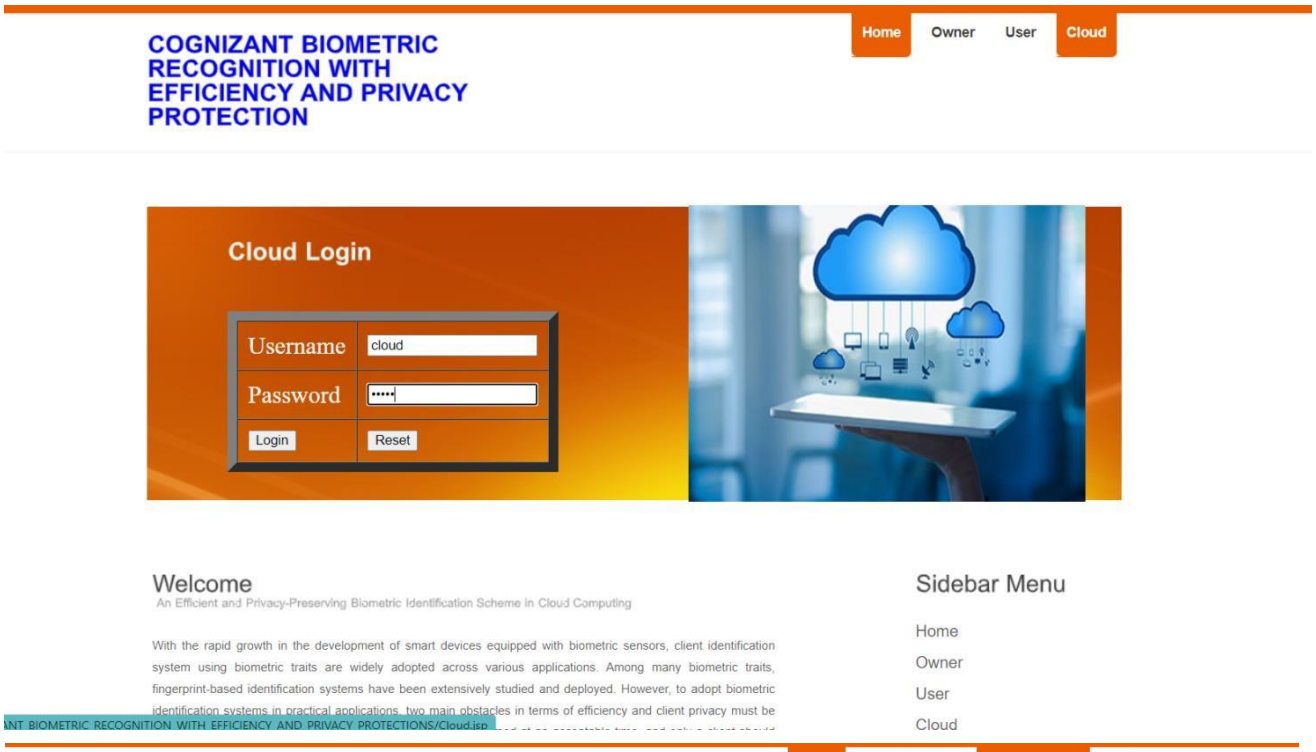


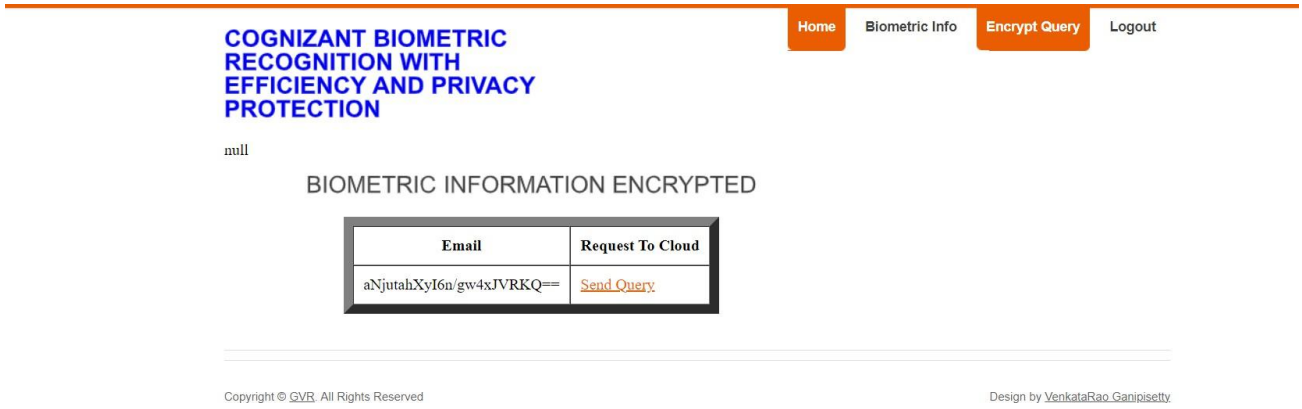


7.6 User Biometric information

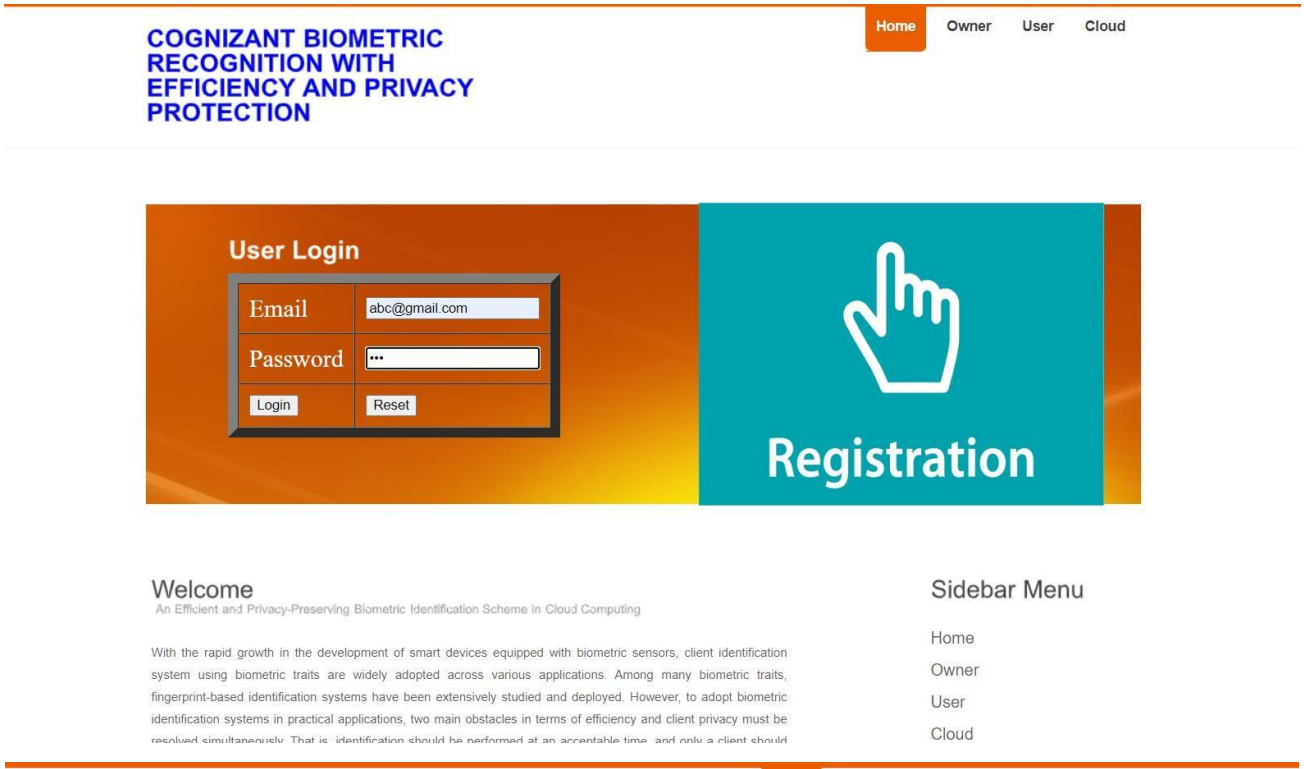


7.7 User query request

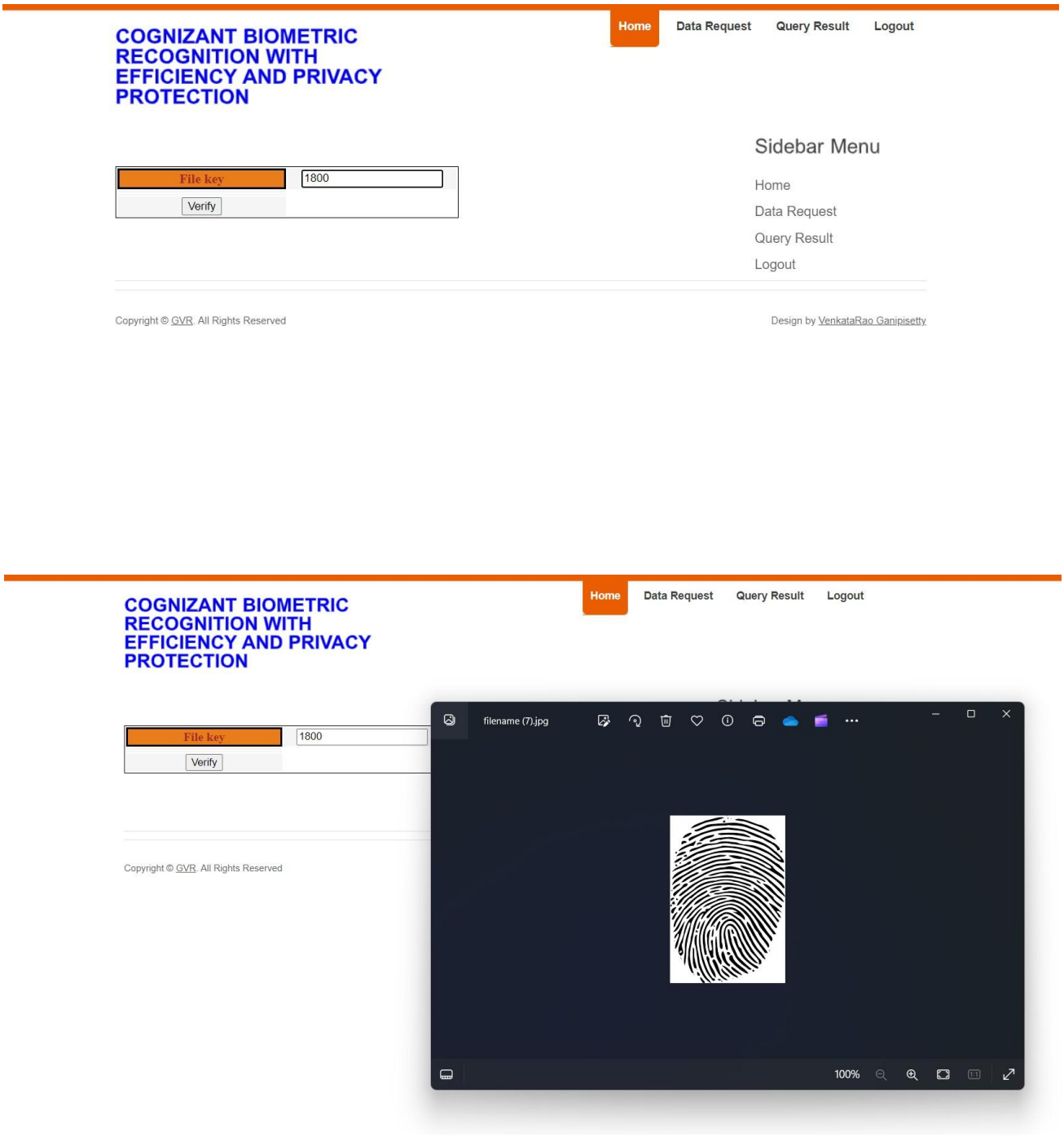




7.8 Encrypt query



7.9 User Login & Key Generation



7.10 Verification &Generation of user Biometric

COGNIZANT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION

Home | Biometric Info | Encrypted | User Request | Logout

BIOMETRIC INFORMATION ENCRYPTED

UserID	Name	Email	Gender	Address
1	3+vF68xrVV4NJ/pX1bUFtw==	N1CLZHuzn5gteQ8LI9fQdGrgPPLR15LpbfXH0WJFcDQ=	lpWZymcwMFFxqw5V0LOqCw==	lpWZymcwMFFxqw5V0LOqCw==

Back

COGNIZANT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION

Home | Biometric Info | Encrypted | User Request | Logout

Welcome To Owner Page

COGNIZANT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION

With the rapid growth in the development of smart devices equipped with biometric sensors, client identification system using biometric traits are widely adopted across various applications. Among many biometric traits, fingerprint-based identification systems have been extensively studied and deployed. However, to adopt biometric identification systems in practical applications, two main obstacles in terms of efficiency and client privacy must be resolved simultaneously. That is, identification should be performed at an acceptable time, and only a client should have access to his/her biometric traits, which are not revocable if leaked. Until now, multiple studies have demonstrated successful protection of client biometric data; however, such systems lack efficiency that leads to excessive time utilization for identification. The most recently researched scheme shows efficiency improvements but reveals client biometric traits to other entities such as biometric database server. This violates client privacy. In this paper, we propose an efficient and privacy-preserving fingerprint identification scheme by using cloud systems. The proposed scheme extensively exploits the computation power of a cloud so that most of the laborious computations are performed by the cloud service provider. According to our experimental results on an Amazon EC2 cloud, the proposed scheme is faster than the existing schemes and guarantees client privacy by exploiting symmetric homomorphic encryption. Our security analysis shows that during identification, the client fingerprint data is not disclosed to the cloud service provider or fingerprint database server. Read more...

Sidebar Menu

Home
Biometric Info
Encrypted
User Request
Logout

8. CONCLUSION

In this paper, we proposed a novel privacy-preserving biometric identification scheme in the cloud computing. To realize the efficiency and secure requirements, we have designed a new encryption algorithm and cloud authentication certification. The detailed analysis shows it can resist the potential attacks. Besides, through performance evaluations, we further demonstrated the proposed scheme meets the efficiency need well.

9. FUTURE SCOPE

The future of biometric recognition is poised for significant advancements, with a strong emphasis on enhancing both privacy and security. Innovations such as homomorphic encryption and secure multi-party computation are paving the way for privacy-preserving biometrics, allowing data to be processed without exposing raw information. Additionally, AI-driven algorithms are improving the accuracy and adaptability of biometric systems, making them more reliable. Multi-modal biometrics, which combine multiple traits like face, voice, and fingerprint, offer robust authentication methods that increase security and accuracy. Continuous authentication, enabled by real-time monitoring of user behavior and biometrics, provides dynamic security measures that adapt to potential threats. Furthermore, decentralized technologies like blockchain are being explored to create secure and transparent platforms for managing biometric data. As biometric technologies continue to evolve, there will be a growing focus on establishing ethical guidelines and regulatory frameworks to ensure responsible use and protect user rights.

10. REFERENCES

[1] A. Jain, L. Hong and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 43, no. 2, pp. 90-98, 2000.

[2] R. Allen, P. Sankar and S. Prabhakar, "Fingerprint identification technology," Biometric Systems, pp. 22-61, 2005.

[3] J. de Mira, H. Neto, E. Neves, et al., "Biometric-oriented Iris Identification Based on Mathematical Morphology," Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195, 2015.

[4] S. Romdhani, V. Blanz and T. Vetter, "Face identification by fitting a 3d morphable model using linear shape and texture error functions," in European Conference on Computer Vision, pp. 3-19, 2002.

[5] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Journal of Computer Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.

[6] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 24-34, 2007.

[7] X. Du and H. H. Chen, "Security in wireless sensor networks," IEEE Wireless Communications Magazine, vol. 15, no. 4, pp. 60-66, 2008.

[8] X. Hei, and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergency," in Proc. of IEEE INFOCOM 2011, pp. 346-350, 2011.

[9] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in Proc. of IEEE GLOBECOM 2010, pp. 1-5, 2010.

[10] M. Barni, T. Bianchi, D. Catalano, et al., "Privacy-preserving fingercode authentication," in Proceedings of the 12th ACM workshop on Multimedia and security, pp. 231-240, 2010.

[11] M. Osadchy, B. Pinkas, A. Jarrous, et al., "SCiFI-a system for secure face identification," in Security and Privacy (SP), 2010 IEEE Symposium on, pp. 239-254, 2010.

[12] D. Evans, Y. Huang, J. Katz, et al., "Efficient privacy-preserving biometric identification," in Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS, 2011.

[13] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in Proc. of IEEE INFOCOM 2013, pp. 2652-2660, 2013.

[14] Q.Wang, S. Hu, K. Ren, et al., "CloudBI: Practical privacy-preserving outsourcing of biometric identification in the cloud," in European Symposium on Research in Computer Security, pp. 186-205, 2015.

[15] Y. Zhu, Z.Wang and J.Wang, "Collusion-resisting secure nearest neighbour query over encrypted data in cloud," In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on, pp. 1-6, 2016.

[16] S. Pan, S. Yan, and W. Zhu, "Security analysis on privacy-preserving cloud aided biometric identification schemes," in Australasian Conference on Information Security and Privacy, pp. 446-453, 2016.

[17] C. Zhang, L. Zhu and C. Xu, "PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud," Information Sciences, vol. 409, pp. 56-67, 2017.

[18] Y. Zhu, T. Takagi, and R. Hu, "Security analysis of collusion-resistant nearest neighbor query scheme on encrypted cloud data," IEICE Transactions on Information and Systems, vol. 97, no. 2, pp. 326-330, 2014.

[19] A. Jain, S. Prabhakar, L. Hong, et al., "Filterbank-based fingerprint matching," IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846-859, 2000.

[20] H. Delfs, H. Knebl, and H. Knebl, "Introduction to cryptography," Berlin etc.: Springer, 2002.

[21] K. Liu, C. Giannella, and H. Kargupta, "An attacker's view of distance preserving maps for privacy preserving data mining," Knowledge Discovery in Databases, pp. 297-308, 2006.

[22] Y. Wang, and D. Hatzinakos, "Face recognition with enhanced privacy protection," in IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 885-888, 2009.

[23] K.Wong, and M. Kim, "A privacy-preserving biometric matching protocol for iris codes verification," in Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), pp. 120-125, 2012.

[24] W. Wong, D. Cheung, B. Kao B, et al., "Secure kNN computation on encrypted databases," in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, pp. 139-152, 2009.