COGNIZANT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION

[1] Mrs.K.Bhavana,[2] G.Anusha,[3] G.Jeevanraj,[4] K.Maneesha,[5] K.Hemanth
[1] Assistant Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

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 this paper, we propose an efficient and privacypreserving biometric identification outsourcing scheme. Specifically, the biometric data is encrypted and outsourced to the cloud server. To execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over the encrypted database and returns the result to the database owner. A thorough security analysis indicates the proposed scheme is secure even if 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 and identification procedures.

I. INTRODUCTION

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.

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.

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.

Services Models:

Cloud Computing comprises three different service models, namelyInfrastructure-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 she accesses a service on the application layer, these tasks are normally taken care of by thecloud service provider.

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.

II. LITERATURE SURVEY

1. TITLE: Privacy-preserving finger code authentication.

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

ABSTRACT: We present a privacy preserving protocol for fingerprint-based 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 biometric 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 Finger code, 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 finger code 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 fingerprint-based system, they can be generalized to any biometric system that shares the same matching methodology, namely distance computation and thresholding.

TITLE: Efficient privacy-preserving biometric identification

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

ABSTRACT: 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.

TITLE: Collusion-resisting secure nearest neighbor query over encrypted data in cloud

AUTHORS: Youwen Zhu ; Zhikuan Wang ; Jian Wang

ABSTRACT: 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.

TITLE: Security analysis on privacy-preserving cloud aided biometric identification schemes

AUTHORS: Youwen Zhu ; Zhikuan Wang ; Jian Wang

ABSTRACT: 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.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

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.

DISADVANTAGES:

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.

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 insufficiency 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.

SYSTEM ARCHITECTURE

----------REMAINING----------

Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- **OWNER**
- **USER**
- **CLOUD**

MODULE DESCRIPTION

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 cipher text for the biometric trait and then transmits the cipher text 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. When we talk about cognizant biometric recognition, we're looking at systems that use biometric data like fingerprints, facial recognition, or iris scans to identify individuals. The goal here is to make the recognition process smarter and more aware of the context in which it's used.Efficiency in biometric recognition involves making the identification process quick and accurate. This can be achieved through advanced algorithms, hardware optimization, and streamlined processes to ensure that the recognition is fast and reliable.Now, when it comes to privacy protection for the owner module, it's about safeguarding the biometric data and ensuring that the owner has control over who can access and use their biometric information. By combining cognizant biometric recognition with efficient processes and robust privacy protection for the owner module, we can create a system that not only accurately identifies individuals but also respects their privacy and security.

DATA USER

When a user wants to identify himself/herself, a query request is be sent to the database owner. In the context of the user module, efficiency in biometric recognition aims to make the user experience smooth and seamless. This involves ensuring that the biometric authentication process is quick, reliable, and user-friendly. Technologies like machine learning and AI can enhance the efficiency of biometric recognition systems by continuously improving recognition accuracy and speed.When it

Comes to privacy protection for the user module, it's crucial to prioritize the security and confidentiality of the user's biometric data. Measures such as data encryption, secure transmission protocols, and strict access controls can help safeguard the user's biometric information from unauthorized access or misuse. By integrating cognizant biometric recognition with efficient user- centric processes and robust privacy protection measures, we can create a system that not only provides accurate identification but also prioritizes user experience and data security.

Cloud Server:

The cloud server figures out the best match for the encrypted query and returns the related index to the database owner. When we talk about the cloud module in biometric recognition systems, we're referring to the part of the system that stores and processes biometric data in the cloud. Efficiency in the cloud module involves optimizing data storage, retrieval, and processing to ensure quick and accurate recognition.

Technologies like cloud computing, edge computing, and distributed databases can enhance the efficiency of biometric recognition systems in the cloud.

Privacy protection in the cloud module is crucial to safeguarding the sensitive biometric data stored and processed in the cloud. Measures such as encryption, secure communication protocols, data anonymization, and regular security audits can help protect biometric data from unauthorized access or breaches.

By combining cognizant biometric recognition with efficient cloud-based processes and robust privacy protection measures, we can create a system that not only provides accurate identification but also ensures the security and privacy of biometric data stored in the cloud.

V. SCREENSHOTS:

FIG-1

FIG-2

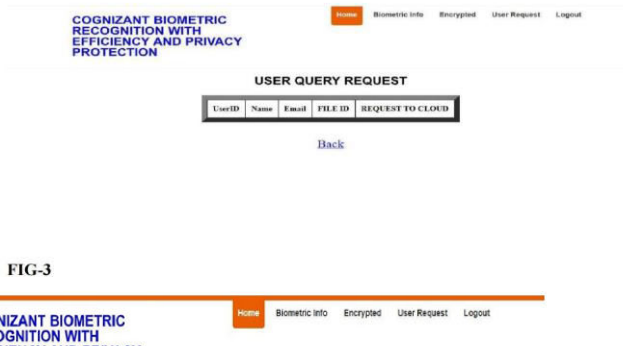
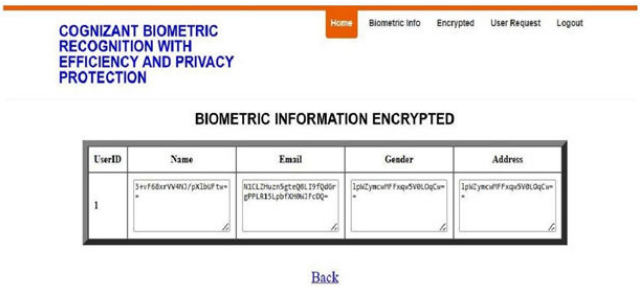


FIG-3



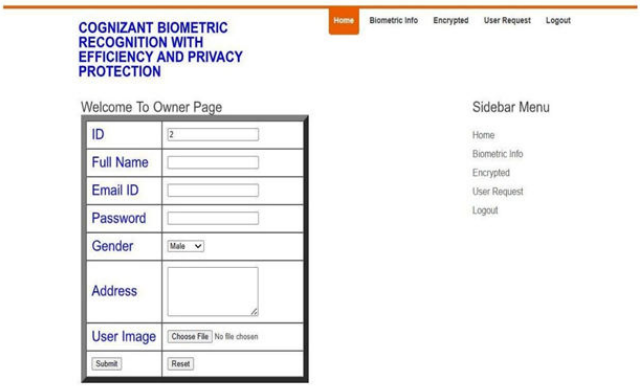


FIG-4

FIG-5

VI. 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.Biometric recognition technology has emerged as a powerful and innovative tool in the field of identity verification and access control. This technology leverages unique physiological and behavioral characteristics of individuals, such as fingerprints, facial features, iris patterns, and voice, to accurately and securely identify and authenticate users.In conclusion, biometric recognition offers several advantages over traditional authentication methods. Its non-intrusive nature, speed, and accuracy make it a compelling choice for a wide range of applications, from unlocking smartphones to securing sensitive facilities. The continuous advancements in biometric technology, including the integration of artificial intelligence and machine learning, contribute to its evolving effectiveness and reliability.

FUTURE SCOPE

The future scope of biometric recognition is poised for significant advancements and widespread integration across various domains. With ongoing research and development, biometric technologies are expected to become more sophisticated, accurate, and versatile. Emerging modalities such as behavioral biometrics, including gait and keystroke dynamics, are likely to complement traditional physiological measures like fingerprints and facial recognition, enhancing overall security and authentication systems. Moreover, the integration of artificial intelligence and machine learning algorithms will contribute to continuous improvement in biometric systems, making them more adaptive to evolving threats and capable of handling large-scale applications. The proliferation of biometric recognition in areas such as finance, healthcare, and smart cities indicates a transformative impact on security, convenience, and efficiency in the future landscape. However, ethical considerations and privacy concerns will also play a crucial role in shaping the responsible deployment of these technologies.

REFERENCES

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

1. R. Allen, P. Sankar and S. Prabhakar, “Fingerprint identification technology,” Biometric Systems, pp. 22-61, 2005.

2. 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.

3. 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,
4. 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,
10. 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 andPrivacy (SP), 2010 IEEE Symposium on, pp. 239254, 2010.