



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

Efficient Privacy-Preserving Biometric Identification in Cloud Computing

Bala Kumar R S¹, Sujitha R²

¹Student (Department of MCA, Narayanaguru College of Engineering, Anna University)

²Assistant Professor, (Department of MCA, Narayanaguru College of Engineering, Anna University)

ABSTRACT

Benefited from its reliability and convenience, biometric identification has become one of the most popular authentication technologies. Due to the sensitivity of biometric data, various privacy-preserving biometric identification protocols have been proposed. However, the low computational efficiency or the security vulnerabilities of these protocols limit their wide deployment in practice. To further improve the efficiency and enhance the security, in this project, propose two new privacy-preserving biometric identification outsourcing protocols. One mainly utilizes the efficient Householder transformation and permutation technique to realize the high-efficiency intention under the known candidate attack model. The other initializes a novel random split technique and combines it with the invertible linear transformation to achieve a higher security requirement under the known-plaintext attack model. Also, argue the security of our proposed two protocols with a strict theoretical analysis and, by comparing them with the prior existing works, comprehensively evaluate their efficiency.

Keywords: Biometric identification, privacy-preserving, householder transformation, cloud computing.

1 Introduction

Biometric identification uses a person's unique physical traits such as their iris, voice, face, fingerprints or behavioral features-such as gait, voice, keystrokes to authenticate, verify and identify them. Compared to traditional authentication methods (such as passwords or smart cards), biometrics cannot be lost, forgotten or stolen. As Schneier has said: "You are your key" [18]. Therefore, biometrics are easy to use and empower a seamless, frictionless user experience. Currently, biometric identification is widely used in government agencies and private enterprises, as well as organizations requiring access control and employee identification such as electronic health [11], industrial internet of things [12], wireless sensor networks [15], assistive robots [16]. Noteworthy, as Research and Markets Ltd. reported, the use of contactless biometric systems has greatly increased due to the spread of COVID-19 [21]. Generally, the biometric identification involves a dataset of biometrics and a query. The data owner (DO) performs a search task over the dataset to match the query data. However, in the current big data era, the quantity of biometric data is growing in an exponential speed, which



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

causes heavy storage and computational burdens on the DO. Therefore, outsourcing the storage and the identification task to a cloud server has become a popular computing diagram. Within this diagram, a resource-constrained DO can enjoy the abundant storage and computational resource on a pay-as-you-demand manner. Although cloud-assisted biometric identification has been shown a promising application foreground in practice, it also faces several serious security challenges. On the DO side, due to the sensitivity of biometrics, the leakage and abuse of these data may lead to inestimable loss of life and properties [17]. On the cloud side, for outside financial incentives, it may be curious about DO's privacy information and deliberately reveal these data to malicious attackers. Therefore, a well-designed biometric identification outsourcing protocol should ensure the privacy of DO's sensitive data. Meanwhile, since DO needs to spend additional cost to protect the privacy information, the privacy-preservation approach must be efficient. That is, compared with achieving the identification task by the DO itself (without outsourcing), the designed outsourcing protocol also should ensure the DO to gain decent computational savings. Consequently, designing efficient and privacy-preserving biometric identification outsourcing protocols becomes a hot topic.

2 Related Works

[1] Efficient and privacy-preserving biometric identification in cloud, Changhee Hahn-2020. 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 show 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.

[2] Efficient Privacy-Preserving Biometric Identification in Cloud Computing Jiawei Yuan-2019. Biometric identification is a reliable and convenient way of identifying individuals. The



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

widespread adoption of biometric identification requires solid privacy protection against possible misuse, loss, or theft of biometric data. Existing techniques for privacy-preserving biometric identification primarily rely on conventional cryptographic primitives such as homomorphic encryption and oblivious transfer, which inevitably introduce tremendous cost to the system and are not applicable to practical large-scale applications. In this paper, we propose a novel privacy-preserving biometric identification scheme which achieves efficiency by exploiting the power of cloud computing. In our proposed scheme, the biometric database is encrypted and outsourced to the cloud servers. To perform a biometric identification, the database owner generates a credential for the candidate biometric trait and submits it to the cloud. The cloud servers perform identification over the encrypted database using the credential and return the result to the owner. During the identification, cloud learns nothing about the original private biometric data. Because the identification operations are securely outsourced to the cloud, the realtime computational/communication costs at the owner side are minimal. Thorough analysis shows that our proposed scheme is secure and offers a higher level of privacy protection than related solutions such as kNN search in encrypted databases. Real experiments on Amazon cloud, over databases of different sizes, show that our computational/communication costs at the owner side are several magnitudes lower than the existing biometric identification schemes

[3] Privacy preserving security using biometrics in cloud computing Santosh Kumar-2020. Cloud computing and the efficient storage provide new paradigms and approaches designed at efficiently utilization of resources through computation and many alternatives to guarantee the privacy preservation of individual user. It also ensures the integrity of stored cloud data, and processing of stored data in the various data centers. However, to provide better protection and management of sensitive information (data) are big challenge to maintain the confidentiality and integrity of data in the cloud computation. Thus, there is an urgent need for storing and processing the data in the cloud environment without any information leakage. The sensitive data require the storing and processing mechanism and techniques to assurance the privacy preservation of individual user, to maintain the data integrity, and preserve confidentiality.

[4] Privacy-Preserving Biometric Authentication: Challenges and Directions, Elena Pagnin-2020. An emerging direction for authenticating people is the adoption of biometric authentication systems. Biometric credentials are becoming increasingly popular as a means of authenticating people due to the wide range of advantages that they provide with respect to classical authentication methods (e.g., password-based authentication). The most characteristic feature of this authentication method is the naturally strong bond between a user and her biometric credentials. This very same advantageous property, however, raises serious security and privacy concerns in case the biometric trait gets compromised. In this article, we present the most challenging issues that need to be taken into consideration when designing secure and privacy-preserving biometric authentication protocols. More precisely, we describe the main



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

threats against privacy-preserving biometric authentication systems and give directions on possible countermeasures in order to design secure and privacy-preserving biometric authentication protocols.

[5] Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment Tanesh Kumar. Recent developments in Internet of Things (IoT) technologies have already put a huge impact on the medical and health sector. Thus, the patient treatment can be performed in more efficient ways compared with traditional methods. Secure identification is a key system requirement for patients to acquire these health related services. Fast and convenient identification is important in the case of critical and elderly or disabled patients who required frequent health services. In this paper, we are presenting concept of the Naked environment where patients can get health services from smart and intelligent surroundings of hospital without using explicit gadgets. Patients would have direct interaction with the environment and get identified through it. We propose a biometric based authentication scheme for the naked hospital environment that also protects the patient's identity privacy. In addition, we show that this authentication scheme can resist various well known attacks such as insider attacks, replay attacks and identity privacy among others.

3 Proposed Work

We reinvestigate the study of privacy-preserving biometric identification outsourcing protocols and, to better balance the security and efficiency and provide more alternatives, we propose two new cloud-assisted biometric identification protocols. One mainly focuses on high efficiency with decent security model and the other seeks high security with admissible efficiency. Precisely, our main contribution can be summarized as follows.

Firstly, we propose a high-efficiency privacy-preserving biometric identification outsourcing protocol. The key technique ingredient underlying our design is the employment of the efficient Householder transformation, which can reduce the time-consuming matrix-matrix multiplication to efficient matrix-vector multiplication and make our first protocol highly efficient. Also, we argue the security of the protocol under the known candidate attack model. Secondly, we propose a high-security biometric identification outsourcing protocol. Through a newly raised random split technique and the invertible matrix transformation, we realize the privacy preservation of the dataset and the query under the KPA model. Also, the efficiency of this protocol is comparable to the prior works.

Finally, we present a comprehensive evaluation on our two proposed outsourcing protocols by theoretically and experimentally comparing them with the prior existing works. Our theoretical and experimental analysis demonstrates that (1) both of our proposed protocols enable the DO to gain decent computational savings, (2) our protocol I is most efficient among these protocols and (3) our protocol II is more efficient in most of the stages than prior arts.



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

3.1 Advantages of Proposed System

Improved Security: Biometric identification systems can provide a high level of security for user authentication, and using the cloud can provide additional security measures such as encryption and secure data storage.

Scalability: Cloud-based biometric identification systems can be easily scaled up or down to meet changing demands without requiring significant hardware or software investments.

Cost-Effectiveness: Cloud-based systems can be more cost-effective than on-premise solutions, as they do not require significant upfront investments in hardware and infrastructure.

Privacy Preservation: Privacy preservation techniques can be used to protect user privacy in cloud-based biometric identification systems, ensuring that sensitive biometric data is not compromised.

Improved Efficiency: Efficient biometric identification techniques can improve the speed and accuracy of identification processes, reducing wait times and improving the overall user experience.

3.2 System Architecture

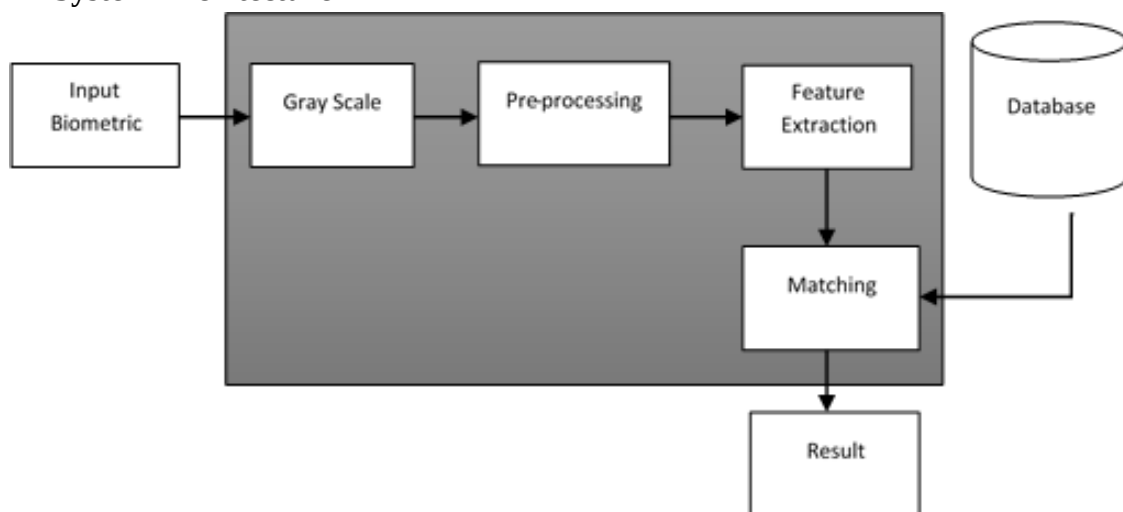


Figure 1: *Biometric frame work*

Feature extraction: Once the biometric data is captured, the feature extraction component processes the data to extract the relevant features. These features are unique to each individual and can be used to distinguish one individual from another.

Template generation: The features extracted from the biometric data are used to create a template, which is a digital representation of the biometric data. The template is stored in a database for later use.

Matching: When a user presents their biometric data, the matching component compares the features of the newly captured biometric data with the templates stored in the database to find a match. The matching process involves a comparison of the similarity of the features of the



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

newly captured biometric data with those in the database. If a match is found, the system identifies the user.

Decision making: The decision-making component decides whether the newly captured biometric data is a match or not. The decision is based on a threshold value, which determines the minimum level of similarity required to consider a match.

3.3 Modules

Load Biometric: It's important to note that the availability of biometric modules may vary depending on the specific biometric modality and the purpose of your identification system. There are numerous biometric software development kits (SDKs) and APIs available from various vendors that provide pre-built modules for biometric identification. Some popular biometric technology providers include Neurotechnology, Innovatrics, Aware, and Idemia.

Gray Scale Process: To achieve efficient biometric identification, a crucial step is pre-processing the biometric data, particularly when working with grayscale images. Preprocessing helps enhance the quality and reliability of the biometric data, leading to improved identification accuracy.

Edge Detection: An edge detection module is a critical component of a biometric identification system, especially when working with images or video frames. Edge detection helps in identifying and extracting the boundaries or edges of objects or features within an image, which can be crucial for accurate feature extraction and subsequent matching.

Feature Extraction: A feature extraction module is a crucial component of an efficient biometric identification system. It processes the pre-processed biometric data and extracts relevant and distinctive features that represent the unique characteristics of individuals. These features are then used for comparison and matching during the identification process.

Fingerprint Matching: Template Generation: Convert the extracted features into a compact template that represents the fingerprint. The template should be stored efficiently and allow for fast matching. Common template formats include minutiae templates, ridge-based templates, or hybrid templates that combine different feature representations.

4 Result and Discussion

The results section presents the outcomes of the efficient biometric identification system. It includes quantitative metrics such as identification accuracy, false acceptance rate (FAR), and false rejection rate (FRR). The results are compared with existing biometric identification systems to assess the efficiency and effectiveness of the proposed approach. Additionally, the section discusses the impact of various parameters, such as the size of the biometric database and computational resources, on system performance.

The discussion section analyse and interprets the results obtained from the experiments. It explores the implications of the findings and provides insights into the efficiency and privacy preservation aspects of the proposed system. Furthermore, this section highlights the



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

advantages and limitations of the system and suggests potential avenues for future research and improvement.

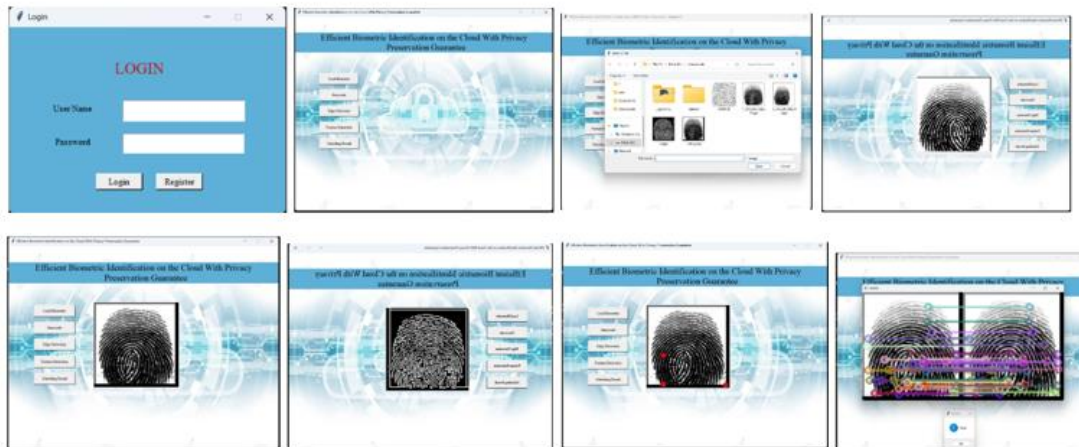


Figure 2: Result of Application Interface

5 Conclusion

In this paper, we design two biometric identification outsourcing protocols for different security and efficiency requirements. With rigorous theoretical argument and extensive experimental analysis, we comprehensively evaluate the security and efficiency of the proposed protocols. Our analysis indicates that our protocols can achieve decent security or efficiency advantages compared with the existing outsourcing protocols

6 Future Enhancement

Efficient biometric identification is an area of active research and development, with ongoing efforts to improve the accuracy, speed, and security of biometric systems. Here are some potential future enhancements for efficient biometric identification: Multi-modal biometrics: Using multiple biometric modalities (such as face, iris, and fingerprint) can improve the accuracy of biometric identification by reducing the false acceptance rate and false rejection rate. Deep learning: Deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can be used to learn complex feature representations and improve the accuracy of biometric identification.

References

1. Yuan Jiawei; Shucheng Yu, Year: 2013, "Efficient privacy-preserving biometric identification in cloud computing," in Proc. IEEE Conf. Comput. Commun. (INFOCOM), pp. 2652–2660.



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

2. Wang Qian; Shengshan Hu; Kui Ren; Meiqi He; Minxin Du; Zhibo Wang, Year: 2015, "CloudBI: Practical privacy-preserving outsourcing of biometric identification in the cloud," in Computer Security, vol. 9327. Cham, Switzerland, pp. 186–205.
3. Liu Chun; Xuexian Hu; Qihui Zhang; Jianghong Wei; Wenfen Liu, Year: 2019, "An efficient biometric identification in cloud computing with enhanced privacy security," IEEE Access, Vol: 7, pp. 105363–105375.
4. Kim Dongmin; Kee Sung Kim, Year: 2021, "A statistical inference attack on privacy-preserving biometric identification scheme," IEEE Access, Vol: 9, pp. 37378–37385.
5. Barni Mauro; Tiziano Bianchi; Dario Catalano; Mario Di Raimondo; Ruggero Donida Labati; Pierluigi Failla; Dario Fiore et al, Year: 2010, "Privacy-preserving fingercode authentication," in Proc. 12th ACM Workshop Multimedia Secur., New York, NY, USA, pp. 231–240.
6. Osadchy Margarita; Benny Pinkas; Ayman Jarrous; Boaz Moskovich, Year: 2010, "SCiFI—A system for secure face identification," in Proc. IEEE Symp. Secur. Privacy, pp. 239–254.
7. Erkin Zekeriya; Martin Franz; Jorge Guajardo; Stefan Katzenbeisser; Inald Lagendijk; Tomas Toft, Year: 2009, "Privacy-preserving face recognition," in Proc. 9th Int. Symp. Privacy Enhancing Technol., vol. 5672. Berlin, Germany: Springer-Verlag, pp. 235–253.
8. Sadeghi Ahmad-Reza; Thomas Schneider; Immo Wehrenberg, Year: 2009, "Efficient privacy preserving face recognition," in Proc. 12th Int. Conf. Inf. Secur. Cryptol., Vol: 5984. Berlin, Germany: Springer-Verlag, 2009, pp. 229–244.
9. Evans David; Yan Huang; Jonathan Katz; Lior Malka, Year: 2011, "Efficient privacy-preserving biometric identification," in Proc. Netw. Distrib. Syst. Secur. Symp., San Diego, CA, USA, pp. 90–98.
10. Zhu Liehuang; Chuan Zhang; Chang Xu; Ximeng Liu; Cheng Huang, Year: 2018, "An efficient and privacy-preserving biometric identification scheme in cloud computing," IEEE Access, Vol: 6, pp. 19025–19033.
11. Aparna Puvvadi; Polurie Venkata Vijay Kishore, Year: 2019, "Biometric-based efficient medical image watermarking in E-healthcare application," IET Image Process., Vol: 13, no: 3, pp. 421–428.
12. Krašovec Andraž; Gianmarco Baldini; Veljko Pejović, Year: 2021, "Opposing data exploitation: Behaviour biometrics for privacy-preserving authentication in IoT environments," in Proc. 16th Int. Conf. Availability, Rel. Secur., New York, NY, USA, pp. 1–7.
13. Zhu Youwen; Zhikuan Wang; Jian Wang, Year: 2016, "Collusion-resisting secure nearest neighbor query over encrypted data in cloud, revisited," in Proc. IEEE/ACM 24th Int. Symp. Quality Service, pp. 1–6.



Article Title: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

14. Pan Shiran; Shen Yan; Wen-Tao Zhu, Year: 2016, "Security analysis on privacy-preserving cloud aided biometric identification schemes," in Proc. Australas. Conf. Inf. Secur. Privacy. Berlin, Germany: Springer-Verlag, pp. 446–453.
15. Das Ashok Kumar, Year: 2017, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," Int. J. Commun. Syst., Vol: 30, no: 1, p. e2933.
16. Baltanas Samuel-Felipe; Jose-Raul Ruiz-Sarmiento; Javier Gonzalez-Jimenez, Year: 2020, "A face recognition system for assistive robots," in Proc. 3rd Int. Conf. Appl. Intell. Syst., New York, NY, USA, Jan. 2020, pp. 1–6.
17. Pagnin Elena; Aikaterini Mitrokotsa, Year: 2017, "Privacy-preserving biometric authentication: Challenges and directions," Secur. Commun. Netw., Vol: 2017, pp. 1–9.
18. Bruce Schneier, Year: 1999, "Inside risks: The uses and abuses of biometrics," Commun. ACM, vol. 42, no. 8, p. 136.
19. Hu Shengshan; Minghui Li; Qian Wang; Sherman SM Chow; Minxin Du, Year: 2018, "Outsourced biometric identification with privacy," IEEE Trans. Inf. Forensics Security, Vol: 13, no: 10, pp. 2448–2463.
20. Wong Wai Kit; David Wai-lok Cheung; Ben Kao; Nikos Mamoulis, Year: 2009, "Secure kNN computation on encrypted databases," in Proc. ACM SIGMOD Int. Conf. Manage. data, New York, NY, USA, pp. 139–152.