Brief Report
Volume 13:6, 2022

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

A Report on Biometric Authentication Scheme

Damon Salvatore*

Department of Biostatistics, Science and Technology of New York, USA

Introduction

Biometric authentication can be roughly divided into two types: client end authentication and remote server authentication. In the first scenario, the remote server keeps the reference biometric data and manages the matching. The user registers his identification details and biometrics at the service provider in a standard biometric-based remote authentication technique. Whenever a user requests self-authentication, a new biometric is provided, which is compared to previously stored biometric data, and a determination is made based on a predetermined threshold.

Description

Since each user's biometrics are frequently linked to his personal information on the central server, it shouldn't be simple for hackers to compromise the server and gain the biometric data for remote biometric systems. This has an impact on how well-liked biometric systems are in society, particularly when biometric information is kept in a centralised database that is open to internal or foreign intrusion. Thus, the security and privacy protection of remote verification should be enhanced by implementing distributed biometric systems, Since each user's biometrics are frequently linked to his personal information on the central server, it shouldn't be simple for hackers to compromise the server and gain the biometric data for remote biometric systems. This has an impact on how well-liked biometric systems are in society, particularly when biometric information is kept in a centralised database that is open to internal or foreign intrusion.

Thus, by developing distributed biometric systems, the security and privacy protection of distant verification should be improved. Where the objective is to guarantee the concepts of identity and transaction privacy, which have just just been established as a new security model for biometric verification, and to detach the storage of biometric data from the service provider. In this paradigm, the user U registers their biometric template to the database DB in cleartext or encrypted form. Additionally, at the service provider SP, U registers his personal data as well as the database storage location index for his biometrics. To authenticate himself, U encrypts his (adjusted) biometric template using a homomorphic encryption scheme and sends this to SP, which retrieves the index of U to be used in a Private Information Retrieval (PIR) protocol between SP and DB. Finally, a decision is made after decryption or in the encryption domain by exploiting the homomorphic properties of the underlying encryption scheme.

Current systems implementing this approach provide provable security in this new model, However, because the biometric templates are encrypted, the cost of database storage rises as a result of ciphertext expansion. Additionally, the use of PIR that is based on number theory is extremely computationally expensive at the DB end. As a result, one must create a secure and effective remote biometric verification technique for a distributed system that reduces the complexity, storage costs, and overall complexity and can therefore be used for large-scale systems. With a new method for storing the biometric features, the multi-factor biometric verification technique we show in this section produces a protocol that is both more secure and effective than the ones now in use. We employ an appropriate signature scheme and the ElGamal encryption algorithm for this purpose. Additionally, a powerful PIR protocol is needed, allowing SP to retrieve a thing from the DB while keeping the thing SP is retrieving a secret.

1. The client sensor CS, service provider SP, database DB, and a human user U with a smart card make up our system's four separate components. Our method is made up of two parts, which are similar to existing authentication schemes: the registration phase and the verification phase. The registration phase, however, differs from existing schemes in terms of structure. In the registration step, the human user U provides CS with their biometrics, and CS uses the codebook Cli that is chosen based on the range information dli of each quantized feature wi in the discrete domain to compute the public parameter PAR 14 D1;... ;Dk.The U smart card has the transformational parameters (li;Di). Then, U registers each transformed quantized feature at a randomly chosen storage address in the database, ij, and registers his unique username ID at the SP. In the smart card, U keeps the index list Index 14 i1;... ; ik encrypted with SP's public key. Here, N stands for the database's size, and is the size of the user's feature vector.

2. In the verification phase, the user U presents its biometrics to CS, which computes the feature vector b0 in the continuous domain. Using the parameters stored in the smart card, CS computes wi ¼ Cli ðw0 i -DiÞDi via the PAR and the codebook Cli for i ¼ 1; ...; k. In practice, li ¼ di as in Sutcu et al. (2006). Using cryptographic techniques, SP communicates with CS and DB to accept or reject the user U using the set overlap as the distance metric, where the threshold t represents the error tolerance in terms of minimal set overlap.

Sampling assumption: In the registration phase, enough number of samples (biometric features) is obtained from each user to assign a codeword ci ACli for the computation of PAR by considering the corresponding range information of each feature separately. The features are always ordered and in N.D. Sarier / Journal of Network and Computer Applications 33 (2010) 268–274 271 ARTICLE IN PRESS continuous domain. The parameters of this transformation (i.e. li;Di) are determined and stored in the user's smart card. We present a new design for remote biometric verification that follows the state-of-the-art security model for biometric authentication systems. Due to the correction of the white noise, our system is robust against the variability of the user biometrics. Besides, a different storage mechanism for the biometric data is introduced, which results in decreased storage costs even in small databases due to the elimination of the ciphertext expansion problem caused by the encrypted template storage and due to the single storage of the common features of different users [1-5].

Conclusion

We present a new design for remote biometric verification that follows the state-of-the-art security model for biometric authentication systems. Due to the correction of the white noise, our system is robust against the variability of the user biometrics. Besides, a different storage mechanism for the biometric data is introduced, which results in decreased storage costs even in small databases due to the elimination of the ciphertext expansion problem caused

***Address for Correspondence:** Damon Salvatore, Department of Biostatistics, Science and Technology of New York, USA, E-mail: salvdam578@edu.in*

Date of Submission: 04 June, 2022, Manuscript No. Jbmbs-22-76966; **Editor assigned:** 06 June, 2022, PreQC No. P-76966; **Reviewed:** 18 June, 2022, QC No. Q-76966; **Revised:** 21 June, 2022, Manuscript No. R-76966; **Published:** 29 June, 2022, DOI: 10.37421/-2155-6180.2022.13.111

by the encrypted template storage and due to the single storage of the common features of different users.

Acknowledgement

We thank the anonymous reviewers for their constructive criticisms of the manuscript. The support from ROMA (Research Optimization and recovery in the Manufacturing industry), of the Research Council of Norway is highly appreciated by the authors.

Conflict of Interest

The Author declares there is no conflict of interest associated with this manuscript.

References

1. Dass, Sarat C., Yongfang Zhu and Anil K. Jain. "Validating a Biometric Authentication System: Sample Size Requirements " *J Biom Biosta* 28 (2006): 1902-1319.
2. Sidek, Khairul Azami, and Ibrahim Khalil. "Enhancement of low sampling frequency recordings for ECG biometric matching using interpolation" *J Biom Biosta* 109 (2013) 13-25.
3. Raunig, David L., Lisa M. McShane, Gene Pennello and Constantine Gatsonis, et al. "Quantitative imaging biomarkers: A review of statistical methods for technical performance assessment." *J Biom Biosta* 24 (2015): 27-67.
4. Wu, Hulin. "Statistical methods for HIV dynamic studies in AIDS clinical trials." *J Biom Biosta* 14 (2005): 171-192.
5. Kontopantelis, Evangelos and David Reeves. "Performance of statistical methods for meta-analysis when true study effects are non-normally distributed: A simulation study" *J Biom Biosta* 21 (2012): 409-426.

How to cite this article: Salvatore, Damon. "A Report on Biometric Authentication Scheme." J Biom Biosta 13 (2022): 111.