Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Edge-centric multimodal authentication system using encrypted biometric templates

Zulfiqar Ali [a], M. Shamim Hossain [b,c,*], Ghulam Muhammad [a,d], Ihsan Ullah [e], Hamid Abachi [d], Atif Alamri [b,c,d]

[a] Digital Speech Processing Group, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[b] Research Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[c] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[d] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[e] Insight Centre for Data Analytics, National University of Ireland, Galway, Ireland

HIGHLIGHTS

- Edge-centric authentication of a person based on multiple biometrics.
- A new method of encryption is proposed and implemented to protect the biometrics.
- Personal portable devices (edges) perform the encryption of biometrics.
- Cloud is responsible for the decryption and authentication of biometrics.
- Speech authentication model is developed by using two different speech features.
- Face authentication model is based on eigenfaces.

ARTICLE INFO

Article history:
Received 15 December 2017
Received in revised form 11 February 2018
Accepted 27 February 2018
Available online xxxx

Keywords:
Cloud computing
Privacy protection
Biometric templates
Encryption
Chaotic system
ORL database

ABSTRACT

Data security, complete system control, and missed storage and computing opportunities in personal portable devices are some of the major limitations of the centralized cloud environment. Among these limitations, security is a prime concern due to potential unauthorized access to private data. Biometrics, in particular, is considered sensitive data, and its usage is subject to the privacy protection law. To address this issue, a multimodal authentication system using encrypted biometrics for the edge-centric cloud environment is proposed in this study. Personal portable devices are utilized for encrypting biometrics in the proposed system, which optimizes the use of resources and tackles another limitation of the cloud environment. Biometrics is encrypted using a new method. In the proposed system, the edges transmit the encrypted speech and face for processing in the cloud. The cloud then decrypts the biometrics and performs authentication to confirm the identity of an individual. The model for speech authentication is based on two types of features, namely, Mel-frequency cepstral coefficients and perceptual linear prediction coefficients. The model for face authentication is implemented by determining the eigenfaces. The final decision about the identity of a user is based on majority voting. Experimental results show that the new encryption method can reliably hide the identity of an individual and accurately decrypt the biometrics, which is vital for errorless authentication.

1. Introduction

The recent development in communication technologies enables the use of computing as a utility. The deployment of high-capacity hardware at the user-facing end is no longer required to run applications and Internet services that need storage, computation, and communication. The cloud can provide the platform for such services and applications by supplying centralized resources in a reliable and cost-effective manner. Moreover, cloud analytics is utilized to analyze industry data by using a range of analytical tools and methods. The process data can then be used to draw conclusions and make decisions. According to the prediction of Gartner, approximately 90% of deployed data will be useless by 2018. Therefore, transmitting only relevant data collected by the

* Corresponding author at: Research Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia.
E-mail address: mshossain@ksu.edu.sa (M.S. Hossain).

https://doi.org/10.1016/j.future.2018.02.040
0167-739X/

IoT to the cloud for analysis is important [1,2]. Deploying the edges of low-cost, low-capacity, and low-performance devices in the designed architecture of an application or service for cloud computing is possible as well. In this manner, the data can be filtered through some intelligent methods, and the features of some deployed services and applications can be enhanced. For instance, with the help of edge analytics, the sensors deployed for traffic monitoring can also be used to send an alert to the fire brigade in case of fire by analyzing the surroundings.

Loss of security in transmitting personal and social data is one of the fundamental problems in cloud computing [3–6]. Numerous smart healthcare systems have been developed to monitor patients in smart homes and cities [7,8]. In these smart systems, the patient's data collected by the IoT are transmitted to health centers for diagnosis. Unauthorized access to such sensitive data may create unavoidable circumstances in someone's personal and professional life. For instance, telemedicine has been successfully applied in various areas of medical fields [9–11]. In all of its types [12], that is, store and send, self-monitoring, and interactive, the patient's data travel through wireless communication to specialists and consultants. If patient data are vulnerable in such applications, such as a cosmetic surgery breach,[1] then the patients may face embarrassments and humiliations. Similarly, biometric authentication is required in some applications, such as remote access to secret data and bank accounts [13]. Therefore, individual data transmitted through wireless channels should be secured to avoid financial losses and job termination [14,15]. The main objective of the present study is to develop a secure biometric authentication system based on encrypted biometric templates.

The identity of a person can be verified in the biometric authentication systems using personal attributes, such as speech [16,17], face [18,19], fingerprints [20,21], palmprint [22,23], gait [24,25], and iris [26,27]. These physiological and behavioral attributes of humans are more reliable in authentication compared with knowledge-based or token-based approaches because these attributes cannot be stolen and are unique for every individual. However, the authentication system based on a single biometric is sometimes unable to recognize a person correctly. Therefore, various multimodal authentication systems based on more than one biometrics have been developed for the accurate authentication of a person. In [28], a multimodal biometric system based on speech, face, and fingerprint is proposed. The system simultaneously uses all biometrics to make the final decision about the identity of a person. Although the authors claim that the multimodal authentication system overcomes the limitations of a single biometric, a comparison of each biometric against the multimodal authentication system is not provided. Therefore, the improvement in the case of the multimodal authentication system cannot be noted. In another study [29], a multimodal authentication system based on speech, face, and fingerprint is analyzed for threshold adjustment to ensure that it performs better than the unimodal biometric system. Then, the computed thresholds are used in score level fusion to reach a final decision about the identity of a user. Ribaric et al. also developed a bimodal verification system using palmprint and face [30]. Their experimental results showed that the performance of the bimodal system is close to the results of palmprint authentication. However, significant improvement is observed when the system is compared with face verification. Overall, improvements of 0.74% and 1.72% are attained for the equal error rate (EER) and total error rate, respectively. A multimodal biometric system based on fingerprint and iris recognition is developed in [31]. For authentication, a person is recognized using the fingerprints and iris, and the final decision about the identity is obtained by performing the AND operation between outputs of fingerprint and iris recognition. The authors did not provide the accuracy for each biometric, and the improvement in the case of bimodal authentication is not mentioned.

Several multimodal biometric systems have been developed using speech as one of the biometrics. Kartik et al. developed a bimodal biometric authentication system using speech and signature [32]. Verification of a speaker is done by extracting the Mel-frequency cepstral coefficients (MFCC) [33] and using vector quantization for pattern matching [33]. The maximum obtained accuracies for clean and noisy speech are 100% and 73.75%, respectively. Meanwhile, the highest accuracies for signature recognition with clean and noisy data are 80% and 72.92%, respectively. In the case of bimodal authentication, the system shows an improvement of 1.25% for noisy data. The authors extended their work in [34], and three biometrics, namely, face, speech, and signatures, are considered to implement the biometric authentication system. In the developed system, a 6% improvement is reported for multimodal authentications, while the accuracies of unimodal authentications using face, speech, and fingerprint are 82.5%, 86.67%, and 92.92%, respectively. Kumar et al. also developed a multimodal biometric system using speech and face images. For speaker verification, MFCC with Gaussian mixture model (GMM) is implemented and an EER of 8% is obtained. Face recognition is conducted using principal component analysis (PCA) and linear discriminant analysis. The obtained EER is 22.87%, an improvement of 1% compared with that in unimodal authentication.

According to the European Union General Data Protection Regulation 2016/679, the biometrics of individuals are sensitive data whose use is protected under privacy protection rights [35]. The biometric template must be protected to avoid any leakage of sensitive data [36]. A number of multi-biometric template protection approaches are listed in [37], yet no method for multimodal biometrics system in the encryption domain has been developed so far. Although a general framework that uses homomorphic encryption for the protection of templates in the multimodal authentication system is proposed in [37], the designed framework is developed for fingerprint and signature verification.

In the present study, an encrypted multimodal biometric system based on speech and face images is proposed. The proposed system authenticates a user remotely through the cloud environment. The biometrics travel via wireless communication for processing, which is risky and makes the data vulnerable. To avoid risks, a new method for biometric encryption is suggested and implemented in the proposed system. Moreover, to optimize computing resources, the biometrics are encrypted by the edges, which is another concern in cloud computing in addition to security [3]. Through the encryption, the transmitted biometrics will not be in the original form but in the encrypted form instead. Therefore, the biometrics will not be exposed to threats of data breach. To investigate the new method of encryption in the proposed multimodal authentication system, a user is verified by using the original and encrypted speech and face. The model for speech authentication is developed using two well-known speech features, MFCC and perceptual linear prediction coefficient (PLP), both of which are used with GMM. By contrast, the model for face recognition is based on eigenfaces and Euclidean distance (EUD). The experimental results indicate that the user identity is properly hidden after the encryption and cannot be disclosed unless it is decrypted. Several experiments are likewise performed to ensure that the new encryption method recovered the identity accurately. The results show no observable difference between the original and decrypted signals. The contributions of this study are summarized as follows:

- A new encryption and decryption method for multi-biometric template protection.

[1] https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments.

Please cite this article in press as: Z. Ali, et al., Edge-centric multimodal authentication system using encrypted biometric templates, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.02.040.