Information Sciences 000 (2017) 1–17

Contents lists available at ScienceDirect

Information Sciences

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

Generating stable biometric keys for flexible cloud computing authentication using finger vein

Zhendong Wu[a,*], Longwei Tian[b], Ping Li[c], Ting Wu[a], Ming Jiang[d], Chunming Wu[e]

[a] School of Cyberspace, Hangzhou Dianzi University, Hangzhou, 310018, China
[b] School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, 310018, China
[c] School of Computer Science, Guangzhou University, Guangzhou, 510006, China
[d] School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, 310018, China
[e] School of Computer Science and Technology, Zhejiang University, Hangzhou, 310058, China

ARTICLE INFO

Article history:
Received 13 March 2016
Revised 29 October 2016
Accepted 31 December 2016
Available online xxx

Keywords:
Cloud computing
Biometric keys
User-authentication
Finger vein
High-dimensional space projection

ABSTRACT

Cloud computing is profoundly changing the way of data storage, transfer and process. User authentication is the first security barrier for cloud computing. However, the security of traditional biometric-template-based authentication technology has been challenged because of the information leakage of biometric templates and insufficient user-key strength, which is limited by the ability of the user to memorize keys. In this paper, we propose a new bio-key generation algorithm named FVHS, which combines the advantages of both biometrics authentication and user-key authentication. It directly generates stable and sufficiently strong bio-key sequences from finger vein biometrics. Based on FVHS, a new framework for cloud computing authentication is presented that provides a more flexible, convenient, and secure user authentication. The key idea of FVHS is that through combining machine learning, biometrics, and cryptography technologies, we can mine a special feature vector from the biometrics space that can be separated and stabilized into a fixed number sequence in a higher-dimensional space. Both a theoretical analysis and experimental verification show that FVHS can extract stable bio-keys from high quality finger vein images. FVHS can extract a finger vein bio-key with a Genuine Accept Rate of more than 99.9%, while the False Accept Rate is less than 0.8% and Equal Error Rate is less than 0.5%. Meanwhile, the security strength can reach 256 bits.

1. Introduction

In recent years, with the rapid growth in network computing power and vastly improved intelligent data processing capabilities, data-centric network services have developed rapidly. Cloud computing is one of the most original network services paradigms, and in this paradigm, there will be a large number of data-centric network applications to serve us such as data sharing [12], data storage [22,33], big data management [3], and medical information systems [45]. For most network services, reliable authentication is the starting point. There are many studies on cloud computing access authentication that

[*] Corresponding author.
E-mail addresses: wzd@hdu.edu.cn (Z. Wu), hnldtlw@126.com (L. Tian), liping26@mail2.sysu.edu.cn (P. Li), wuting@hdu.edu.cn (T. Wu), jmzju@163.com (M. Jiang), wuchunming@zju.edu.cn (C. Wu).

http://dx.doi.org/10.1016/j.ins.2016.12.048
0020-0255/© 2016 Elsevier Inc. All rights reserved.

mainly concentrate on the topic of fine-grained access control servers [19,35,37] for different users. However, because of the limits of human memory, people tend to use only one key to login to all network applications. This behaviour is very vulnerable to social engineering dictionaries, eavesdropping, spoofing, and other network attacks. In the cloud computing environment, how to overcome a user's memory limitations to provide rich, personalized authentication credentials and to manage their documents is an important research topic.

Biometrics, because of its inherent natural connection with the user's identity and no need for key memorization, has been widely studied and used. Biometrics technology has been rapidly adopted in a wide variety of security applications such as electronic and physical access control, electronic commerce, digital rights management, and background checking [40]. If biometric technology can be embedded effectively in cloud computing, a more secure and convenient user authentication scheme can be achieved.

This paper proposes a new cloud security certification scheme by developing a new bio-key generation technology. As shown in Fig. 1(a), a user generally uses a single key to log on to all network services. Moreover, in order to reduce the burden on his or her memory, the key is often relatively simple. However, since individual keys are often generated as regular and simple strings, they are very vulnerable to social engineering attacks. For instance, for large-scale "hit library" attacks, the hit success rate is near 80% [13,28]. If we can extract stable random sequences that are 256 bits in length from biological characteristics and maintain biometrics security, social engineering attacks will lose their effectiveness. By combining the bio-key sequence with the characteristic sequence for a service, a user can be equipped with dedicated keys for each service. The keys do not need to be remembered and can be updated at any time.

We propose a new bio-key generation algorithm that can extract stable bio-key sequences from finger vein patterns. Furthermore, its security strength can reach 256 bits. We then propose an embedded bio-key cloud computing service authentication framework, as shown in Fig. 1(b), that can generate a unique key with sufficient strength for each network service without the need for users to remember it. This framework improves user-key management security and is suitable for the cloud computing era. The contributions of this paper can be summarized as follows:

- We provide a new bio-key generation scheme that directly extracts stable key sequences with sufficient strength from biometrics using machine learning techniques. We implement this scheme for finger veins and prove the effectiveness of the algorithm.
- We design a new cloud computing user-authentication framework. By combining the bio-keys of users and specific characteristics of cloud computing services, the framework provides a unique key with sufficient strength for each cloud computing service as well as a flexible key update process, reducing users' key management burden.

The rest of the paper is organized as follows. Section 2 discusses related work, and Section 3 introduces the finger vein bio-key generation algorithm. In Section 4, we introduce the details of our cloud computing user-authentication framework. A security analysis of the bio-key generation algorithm and framework is described in Section 5. In Section 6, we present the experimental results of the new finger vein bio-key generation algorithm. Finally, our conclusions are drawn in Section 7.

2. Related work

Given the increase in cloud computing services, users usually use only one key to login to all services. Traditional single sign-on (SSO) schemes [1] employ a Passport and OpenID as the solution. OpenID is a decentralized SSO mechanism that has been widely adopted by many Internet service providers such as Yahoo and Google [38]. The OpenID solution can solve the user authentication management problem, but it cannot solve the problem that a user single key is vulnerable to social engineering attacks. Recently, research on access authentication of cloud computing have mainly concentrated on fine-grained access control [26,49], secure data sharing [18,20,25], privacy protection [25,38], and cloud search services [7,46]. Zhou et al. [49] proposed a patient self-controllable multi-level privacy-preserving cooperative authentication scheme, which implements three levels of security and preserves privacy in the distributed healthcare cloud computing systems. Joseph et al. [26] introduced a new fine-grained two-factor authentication scheme for web-based cloud computing services. They presented a mechanism of two-factor authentication using a user key and a lightweight security device. Li et al. [18,20] discussed cloud deduplication and the outsourced revocation problem. They used a convergent key to provide data confidentiality during deduplication. Using a convergence key, they attempted to formally address the problem of authorized data deduplication and proposed a secure hybrid cloud architecture that can solve the problem of deduplication with differential privileges. Liu et al. [25] also proposed a shared authority scheme based on the privacy-preserving authentication protocol (SAPA, Shared Authority based Privacy-preserving Authentication protocol), which enhances a user's shared access security in private using an anonymous access mechanism. Overall, these studies are mostly concerned with server access control and few consider the convenience and safety of user keys. Nevertheless, user key security is the foundation of cloud service security. Fu et al. [7] studied searchable encryption over outsourced data, and introduced a scheme for a personalized multi-keyword ranked search over encrypted data while preserving privacy in cloud computing. Xia et al. [46] presented a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like the deletion and insertion of documents.

Recently, biometrics has been well-studied [6,8,10,31]. There are three main kinds of bio-key schemes: Fuzzy Vault, Fuzzy Commitment, and dynamic bio-key generation.

Please cite this article as: Z. Wu et al., Generating stable biometric keys for flexible cloud computing authentication using finger vein, Information Sciences (2017), http://dx.doi.org/10.1016/j.ins.2016.12.048