International Journal of Service Science, Management, Engineering, and Technology
Volume 11 • Issue 2 • April-June 2020

Bio-CAPTCHA Voice-Based Authentication Technique for Better Security and Usability in Cloud Computing

Omar Ahmed Hedaia, Faculty of Computers and Artificial Intelligence, Benha University, Benha, Egypt
Ahmed Shawish, Faculty of Computers and Information Science, Ain Shams University, Cairo, Egypt
Essam H Houssein, Faculty of Computers and Information, Minya University, Minia, Egypt
Hala Zayed, Computers and Artificial Intelligence, Benha University, Benha, Egypt

ABSTRACT

Cloud computing has gained increased interest in the last few years, where an increasing number of providers are converging to such a promising platform. However, the security issues are still a big concern in the cloud, where authentication is a major one. Much research has been conducted to secure the authentication, where some of them used biometric features (fingerprint, face, and voice, etc.). In general, the biometric authentication techniques have a noticeable advantage compared to the traditional techniques because biometric features are hard to be altered or forged. Nevertheless, a new generation of attacks threatens the biometric security by using brute force approaches. This article proposes a nontraditional authentication technique that was called Bio-CAPTCHA. The proposed technique uses a random voice-based password challenge that dynamically changes every time the user tries to login, which promises to significantly decrease the possibility of unauthorized access. The conducted Experimental and theoretical analysis confirms the high-security level of the proposed technique.

KEYWORDS

Authentication, Biometric, CAPTCHA, Cloud, Security, Voice Recognition

1. INTRODUCTION

Cloud computing brought a lot of advantages such as remote computation, data processing and storing in a way that can be accessed from anywhere using any web-enabled devices (Mlgheit et al., 2017; Banyal et al., 2013). Not to mention that many Cloud services providers standardized their platforms to provide computing resources on-demand without the need for too much administration or configuration. Along with all these advantages, there are still some security concerns that halter the migration of some users to the Cloud (Mlgheit et al., 2018).

The authentication technique is an important factor in the security of the cloud, and it is the first step for protecting the data and the privacy of the user (Velciu et al., 2014). However, Yassin et al. (2012) mentioned that 75% of web applications use the username/password-based authentication technique. those techniques proved the lack of security, due to the fact, that the password can be stolen, lost or even guessed. Therefore, compromising the authentication technique will give the attacker

DOI: 10.4018/IJSSMET.2020040104

the right to use and/or manipulate the users' data. Many authentication techniques use biometrics features due to their uniqueness and being hard to forge (Velciu et al., 2014).

In general, biometric means the use of the biological features to define the user, such as (face, palm print, fingerprint, and voice). Biometric can be categorized into two groups: behavioral and physiological. Behavioral means identifying the user based on his behavior like keystroke and voice, while physiological means identifying the user using his/her physical body features like the fingerprint, iris, etc. Particularly, the voice and speech recognition has met quite an interest in the business field like in (amazon ALEXA, apple SIRI and windows CORTANA).

At this point, the authentication techniques have been classified as Unimodal and Multimodal techniques, where the Unimodal techniques are all the ones that adopt one method for authenticating the user whether it is Biometric-based or non-Biometric, while the Multimodal techniques are those that adopt more than one level of authentication (Gupta, 2017).

Based on a comprehensive review of both Uni/Multi-modal techniques, it is noted that the multi-modal techniques increased the security but on the favor of usability and satisfactory level of the users such in Lupu (2018), Pradhan et al. (2018), Miguel-Hurtado et al. (2017) and Matsuo et al. (2018). This is due to the obligation of using special sensors to acquire the Biometric data like fingerprint sensor, iris sensor, special HD camera, and microphone, which may not be always available on the user side. On the other side, unimodal biometric techniques are based on the assumption that biometrics are secure and can't be stolen like Islam et al. (2009) and Ranjan et al. (2013), which is not always true as proven through numerous of recent attacks. Nevertheless, although the username/password-based authentication technique possesses the highest usability rate, it always suffers from security issues and can be forgotten with the continuous change. The need for an efficient authentication technique featured by both high usability and security becomes crucial especially with the continuous increases in the amount of data on the Cloud.

The biometric that uses the voice of the user as a characteristic for the identification and verification is called voice biometric authentication. Specifically, Voice recognition met an equal interest in the research field for its advantages and scalability. Not to mention, its increasing interest in the market field like in: (telephone banking, call centers, government administration, etc...). Precisely, voice biometric is the exclusive feature for the user that is related to the human vocal tract anatomy, which adds a large spectrum of possibilities, unlike the fingerprint and iris that are constant and easy to be compromised. Moreover, the features of the voice biometrics are unique as the fingerprint features, which can be used to identify and verify the user.

The usage of voice in authentication has not been yet explored as it should be, where new techniques can be proposed to provide more secure advantages for the Cloud users and data protection all over the web.

This paper introduces a new voice-based authentication technique. The technique uses a random voice-based password challenge that dynamically changes every time the user tries to log in. The proposed technique uses CAPTCHA method to provide unpredictability and ambiguity to the authentication process. The main idea of the technique is based on the physical nature of the human voice signal that possesses a wide spectrum of diversity yet holding the unique identity of the person, unlike the other biometric features that are constant and vulnerable to forging. The main contribution of this paper is to introduce a new authentication technique that combines both usability and security using voice identity. The proposed technique has been theoretically and experimentally tested to prove its efficiency and effectiveness.

The conducted Experimental and theoretical analysis of the proposed technique reveals the significant decrease in unauthorized access probability, while it keeps high usability as it depends only on a mic that should be available in most of the web-enabled devices.

The organization of the paper is as follows: Section II reviews the scientific background and related work. Section III introduces the proposed authentication technique. An experimental analysis, theoretical analysis, and discussion are presented in Section IV. Finally, the Conclusion and future work are stated in Section V.