Chapter 5
Efficient Password Mechanism to Overcome Spyware Attack:
Quantum Network and AI

Ajith Peter Vianney R.
Sathyabama Institute of Science and Technology, India

S. Manikandan
https://orcid.org/0009-0000-6693-7873
Sathyabama Institute of Science and Technology, India

A. C. Santha Sheela
https://orcid.org/0000-0003-2466-543X
Sathyabama Institute of Science and Technology, India

ABSTRACT

This study enhances existing authentication systems that use one-time passwords (OTP) and personal identification numbers (PIN) by adding biometric data as a second layer of user authentication. As an alternative to entering the password as normal, users using the recommended method doodle each digit on the touchscreen of the device. The authors conduct a comprehensive evaluation of each handwritten digit's robustness and discriminative ability, along with an assessment of the proposed biometric technique's performance with longer passwords. The e-BioDigit database, comprising handwritten digits 0 through 9, is created using finger input on a mobile device. In summary, the implementation of the suggested technique aimed at enhancing the security of existing PIN and OTP systems has yielded positive outcomes. Specifically, in scenarios where the attacker is already aware of the password, the method demonstrates equal error rates of approximately 4.0%. This

DOI: 10.4018/979-8-3693-9336-9.ch005

stands in stark contrast to traditional PIN and OTP systems, where an impersonation attack would invariably succeed in 100% of cases.

I. INTRODUCTION

This project's primary goal is to create user-friendly mobile applications with strong security and data protection. The quick and widespread adoption of mobile devices across the globe has been spurred not only by the rapid advancement of technology that makes real-time social media use and communication possible, but instead of inputting the password as usual, users in our suggested method sketch each digit on the device's touch screen. Optical Character Recognition, for instance, can be used to initially identify the handwritten numerals, (Salehan & Negahban, 2013).

Most people now consider mobile gadgets to be essential tools. In addition to the rapid advancement of technology and the addition of new features, new network infrastructures like 5G, which enable real-time social media usage and communication, have also contributed to the widespread and rapid deployment of mobile devices worldwide. In this approach, the public and private sectors are attempting to implement their services through user-friendly mobile applications that ensure high security and data protection, acknowledging the significance of mobile devices for society. Historically Personal identification numbers (PINs) and one-time passwords (OTPs) have historically been the two most popular ways to authenticate users. While PIN-based authentication systems need users to learn their own passwords for every use—such as sending messages to personal mobile devices or special tokens—OTP-based authentication systems save users from having to do so.Studies have shown that PIN- and OTP-based authentication methods have shortcomings, even though they are widely used and deployed in real-world settings. Initially, it's customary to utilize passwords that are composed of sequential numbers, private data like birth dates, or easily guessed terms like “password” or “qwerty.” Second, there is a risk of “smudge attacks” when entering passwords on portable devices like tablets or smartphones., i.e., an impostor could be able to guess the password by looking for finger grease residue left on the touchscreen. Finally, “shoulder surfing” can also occur with password-based authentication, (Bonneau, Herley, & Oorschot, 2012).

This kind of assault occurs when the imposter has the ability to watch in person or gather user data via external recording devices. A lot of researchers have been interested in this approach lately because of the growing use of public surveillance systems and handheld recording devices, (Galbally, Coisel, & Sanchez, 2017). High security and ease of use are combined in biometric recognition techniques to overcome these obstacles.