Chapter 4

Multi-Factor Authentication Web Security System Based on Facial Recognition, One Time Password, and Hashed Secure Question

Graveth Uzoma Ejekwu
https://orcid.org/0000-0002-0698-6718
NYSC Secretariat Bayelsa, Nigeria

Samson Ajodo
https://orcid.org/0000-0002-4845-1682
Nigerian Defence Academy, Nigeria

O. Mashood Lawal
https://orcid.org/0000-0002-1312-944X
Air Force Institute of Technology, Nigerian Air Force Base, Mando, Nigeria

Oluwafemi S. Balogun
https://orcid.org/0000-0002-8870-9692
University of Eastern Finland, Finland

ABSTRACT

Web application authentication is a critical aspect of digital security, serving as both the first and last line of defense for safeguarding sensitive information. Unfortunately, traditional text-based passwords are susceptible to a variety of attacks, leaving many web apps vulnerable to data theft by unauthorized users. As a solution, this study developed a multi-factor authentication technique to bolster the conventional username and password method. Utilizing Agile methodology, the proposed solution examined current authentication practices and evaluated the feasibility of multi-factor authentication. The system generates a one-time password (OTP) using the user's login credentials and incorporates additional steps such as face recognition and secure hashed questions for user authentication. To enhance security and user flexibility, the system was implemented using Python programming language, various Python libraries, and an image processing library.

DOI: 10.4018/979-8-3693-1487-6.ch004

1. INTRODUCTION

The world wide web as an entity is been seen my business owners and online vendors and most organizations as a place to carry out businesses and transactions. Individuals and companies perform many tasks on the web such as fetching emails and sending emails, getting access to various gate for making payments of all kinds and also generating reports of various kinds, also having access to contacts information stored on the cloud either google cloud or yahoo cloud via computer systems or mobile phones, this requests are sent through the web browser which in turn returns a response from the host server. Website authentication being the first protective measure for a website user to secure his/her data and to make sure the data is higher secured and restricted from authorized users.

Mostly users navigating the website will need to verify his/her login details, this login details are usually setup at the early stage of creating account with a website or desktop application as well android applications, this verification is done by the user either by statically inputting the login details or automatically inputted by the web browser password manager or google password saver like Authenticator, LastPass etc. This authentication is performed during login process of the website or android applications.

Text-based authentication has been the most common approach used by websites and mobile applications, however this approach or partner of authenticating users is not sufficient enough to provide protection against authorized users from getting information of another user, this is because the approach is open to multiple cyber-attacks example brute force password guessing, phishing attack and the rest of it.

The word authentication is the process or method of confirming a user identity or a request coming from a system that is providing certain types of services to the entity (user) requesting the service. This is done to make sure a user making the request is actually a valid user as they said. In other words, authentication is making sure user supplies the system he/she is making request from with a classified detail agreed between the two entity (user and system) Singh, Charanjeet, & singh, Tripat Deep (2019).

Multi-factor authentication needs more than one verification level to be available. These layers or levels of verification can be user password, which is what the inputted during registration or creating of an account the said system, this is known by the user only on less he or she chooses to share with friends and family, a guarded token or one time password that is sent to user on each login, hashed secure question and Facial Recognition feature. If user provides all the four layers of authentication there will be a higher level of authentication assurance and high level of security, Aldwairi, Monther & Aldhanhani, Saoud (2017, August). The reasons for integrating multiple authentication or security into an application is for the protection of data or what we call data privacy.

Data privacy, this denotes how organizations handle user information or personal information such as transactions, financial data, health records, academic records and many more. Data privacy gives room for organizations to protect user information and keep it from been public else permitted by the said owner of the data. Why data privacy is important, and why every web applications or desktop application should protect customer data from been accessed by unauthorized users.

Knowing fully well that the information mentioned above is important to users and should be kept secret and not be made public, because if this unique identities are compromised it could lead to identity theft or something worse than that, it could lead to user losing their lives or property because their data has been compromised.

Here are some of the reasons why data privacy is important: