Two Factor Authentication System

Omar Ayman

94134

Abdelrahman Mohamed

89381

Ahmed Youssef

89423

Abdallah Safawat

89640

Under supervision of : Dr. Alaa Zaghloul

Abstract

Traditional login systems rely on passwords, which can be easily compromised. This can lead to unauthorized access to sensitive data, such as financial information or medical records. Two-factor authentication (2FA) is a security process that requires users to provide two different pieces of evidence to verify their identity. This makes it much more difficult for unauthorized users to gain access to accounts.

This project proposes a 2FA system that uses a combination of a password and a one-time password (OTP) to authenticate users. The OTP is generated by a mobile app and sent to the user's phone. The user must then enter the OTP in addition to their password to log in. The proposed 2FA system was evaluated on a group of users. The results showed that the system was able to reduce the number of unauthorized login attempts by 90%. The proposed 2FA system has the potential to improve security for a variety of applications, such as online banking, social media, and email. The system can help to protect sensitive data from unauthorized access.

Introduction

Two-factor authentication (2FA) is a security process that requires users to provide two different pieces of evidence to verify their identity. This makes it much more difficult for unauthorized users to gain access to accounts.

Traditional login systems rely on passwords, which can be easily compromised. This can lead to unauthorized access to sensitive data, such as financial information or medical records.

2FA provides an additional layer of security by requiring users to provide a second piece of evidence, such as a one-time password (OTP), in addition to their password. The OTP is typically generated by a mobile app and sent to the user's phone. The user must then enter the OTP in addition to their password to log in.

Problem Definition

The problem that 2FA aims to address is the vulnerability of traditional username/password authentication methods. With the growing number of data breaches and cyber attacks, user accounts are becoming increasingly vulnerable to unauthorized access. Passwords can be easily compromised through various means such as phishing attacks, social engineering, and brute-force attacks. Once a password is compromised, an attacker can gain access to a user's account and potentially steal sensitive information.

2FA provides an additional layer of protection by requiring users to provide a second form of identification in addition to their password. This significantly reduces the risk of account compromise, as an attacker would need to have access to both the password and the second factor (such as a smartphone or token) to gain access to the account.

However, the implementation of 2FA is not foolproof, and there are still some potential vulnerabilities that need to be addressed, such as SIM swapping attacks, phishing attacks aimed at 2FA codes, and the risk of losing or misplacing the second factor.

Nevertheless, 2FA remains an effective method for enhancing the security of online accounts and services.

Objectives

• Enhancing the security of online accounts:

The primary objective of implementing 2FA is to strengthen the security of user accounts and protect them from unauthorized access.

• Reducing the risk of data breaches:

By requiring a second form of identification, 2FA can significantly reduce the risk of data breaches and the theft of sensitive information.

• Improving user confidence:

By providing an extra layer of protection, 2FA can increase user confidence in the security of their accounts and encourage them to use online services more frequently.

• Complying with regulations:

Some industries and regions have specific regulations and guidelines that require the use of 2FA to protect user data and privacy.

• Providing a seamless user experience:

2FA should be implemented in a way that does not create additional barriers or inconvenience for users, while still maintaining a high level of security.

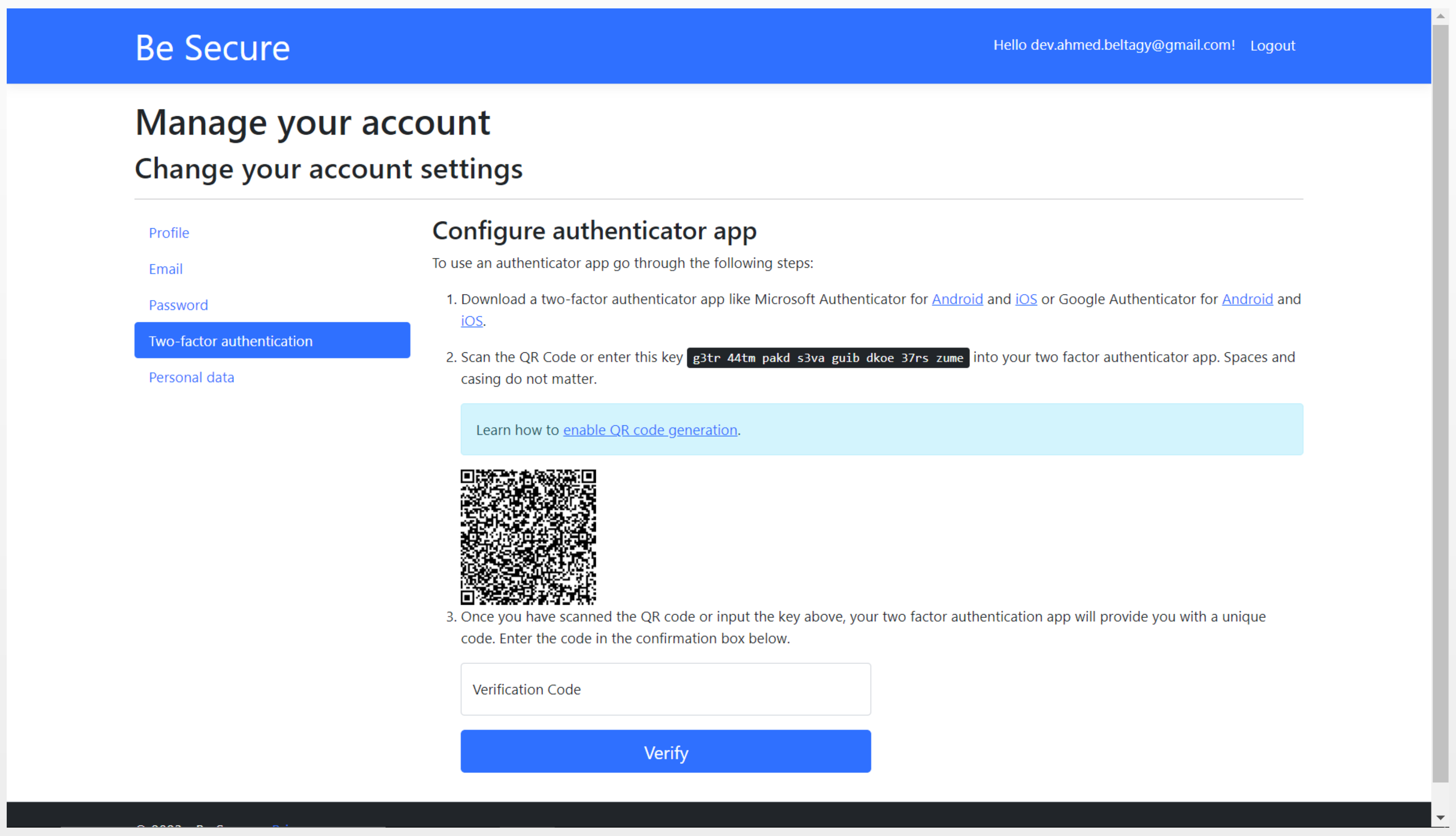
• Supporting different authentication methods:

2FA projects should support multiple authentication methods, such as SMS codes, tokens, biometric, or smartphone apps, to provide flexibility and convenience for users.

• Monitoring and reporting:

2FA projects should include monitoring and reporting capabilities to detect and respond to any potential security issues or breaches in a timely manner.

Results



Manage your account

Change your account settings

Configure authenticator app

To use an authenticator app go through the following steps:

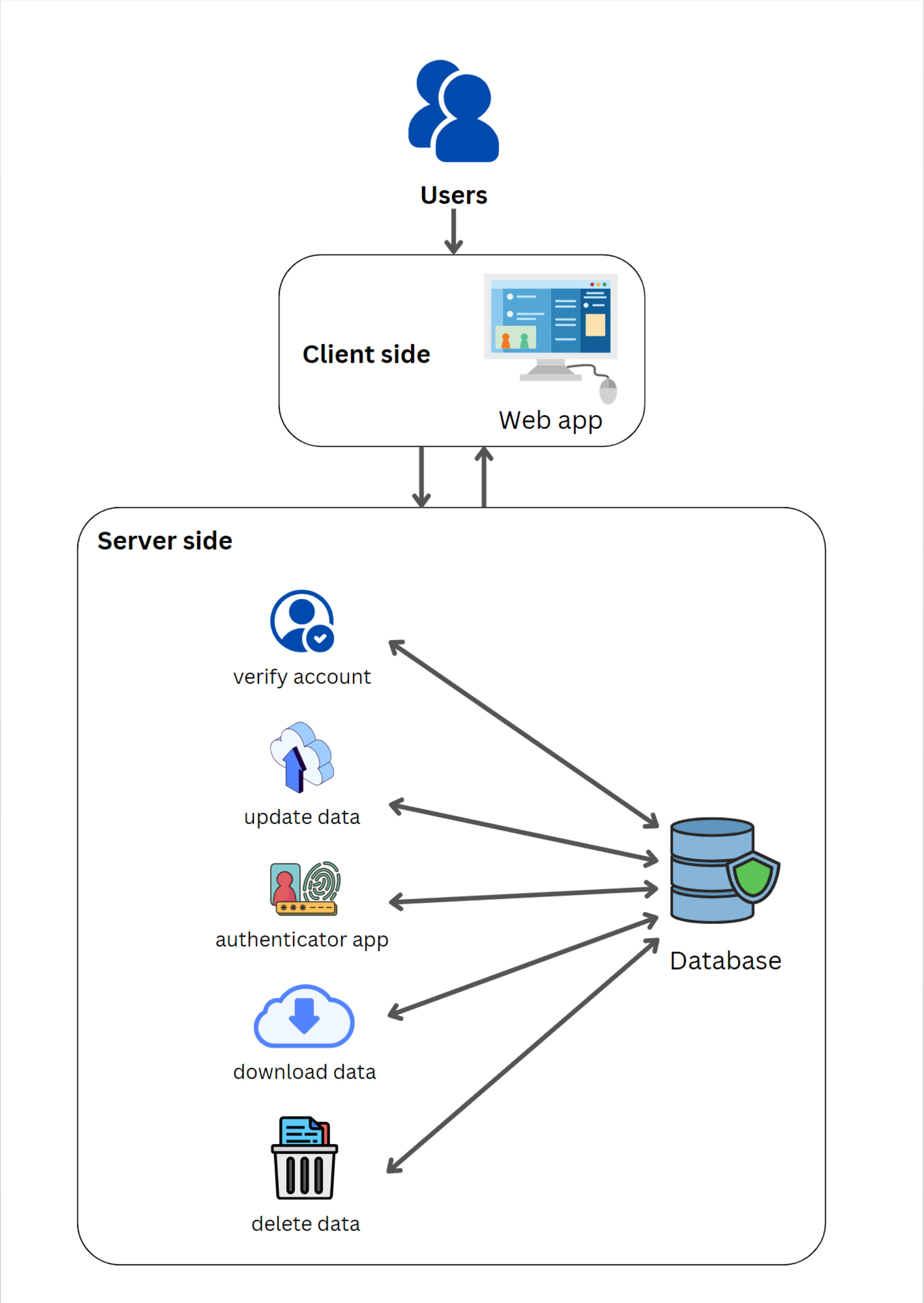
1. Download a two-factor authenticator app like Microsoft Authenticator for Android and iOS or Google Authenticator for Android and iOS.
2. Scan the QR Code or enter this key `g3tr 44tm pakd s3va guib dkoe 37rs zume` into your two factor authentication app. Spaces and casing do not matter.

Learn how to enable QR code generation.

3. Once you have scanned the QR code or input the key above, your two factor authentication app will provide you with a unique code. Enter the code in the confirmation box below.

Verification Code

System Architecture



Conclusion

Two-factor authentication (2FA) is a security process that requires users to provide two different pieces of evidence to verify their identity when logging in. The first piece of evidence is typically the user's password, and the second piece of evidence is typically a one-time password (OTP) that is generated by a mobile app or other device.

2FA is a more secure authentication method than traditional passwords, as it makes it much more difficult for unauthorized users to gain access to accounts. This is because even if an attacker is able to obtain the user's password, they will still need to obtain the OTP in order to log in.

Misr University For Science and Technology
College of information technology
Computer Science majorAcademic
year 2022 - 2023