# Two Factor Authentication

Omar Ayman[1], Abdelrahman Mohamed[2], Ahmed youssef[3], Abdullah safwat[4]

[1]Misr University for Science and Technology

94134@must.edu.eg

[2]Misr University for Science and Technology

89381@must.edu.eg

[3]Misr University for Science and Technology

89423@must.edu.eg

[4]Misr University for Science and Technology

89640@must.edu.eg

## ABSTRACT

Two-factor authentication (2FA) is a security measure that adds an extra layer of protection to online accounts and services. It requires users to provide two forms of identification before they can access their accounts, such as a password and a one-time code sent to their smartphone. 2FA is increasingly being adopted by online service providers as a way to mitigate the risk of account compromise and data breaches. This abstract provides an overview of the concept of 2FA, its benefits, and its implementation in various technologies and applications. It also highlights the importance of 2FA as a key tool for securing online identities and transactions.

**KEYWORDS:** Two-factor authentication; Security; Authentication; Password; Online accounts.

## 1- INTRODUCTION

Two-factor authentication (2FA) is a security process in which a user provides two forms of identification to verify their identity. This process is used to enhance the security of online accounts, applications, and services, by requiring a user to provide two different pieces of information to prove that they are who they claim to be.

Traditionally, the first factor is a password or PIN, while the second factor can be something like a fingerprint scan, a smart card, or a one-time code sent via text message or generated by an authentication app. By requiring two separate factors, 2FA adds an extra layer of security to the authentication process, making it much harder for attackers to gain unauthorized access to a user's account or data.

2FA has become increasingly popular as more and more people rely on online services for work, communication, and entertainment. While it is not foolproof, 2FA is an effective way to protect your accounts from cybercriminals and other unauthorized users.

## 2- METHEDOLOGY

### 1. Analyzing System requirements

We have studied and identified problems of existing system by determines our users and their data and the relations between them and interaction between them and the system.

### 2. Designing the Proposed System

In this phase, we designed a system architecture and data and process diagrams for interaction between users in the application and database.

### 3. Development of the Proposed System

In this phase, we are going to convert the design of proposed system to computer software, which includes computer programming using FLUTTER software tool written in DART, which is intended to handle the administration of FIRBASE, and translating the design specifications into the computer code.

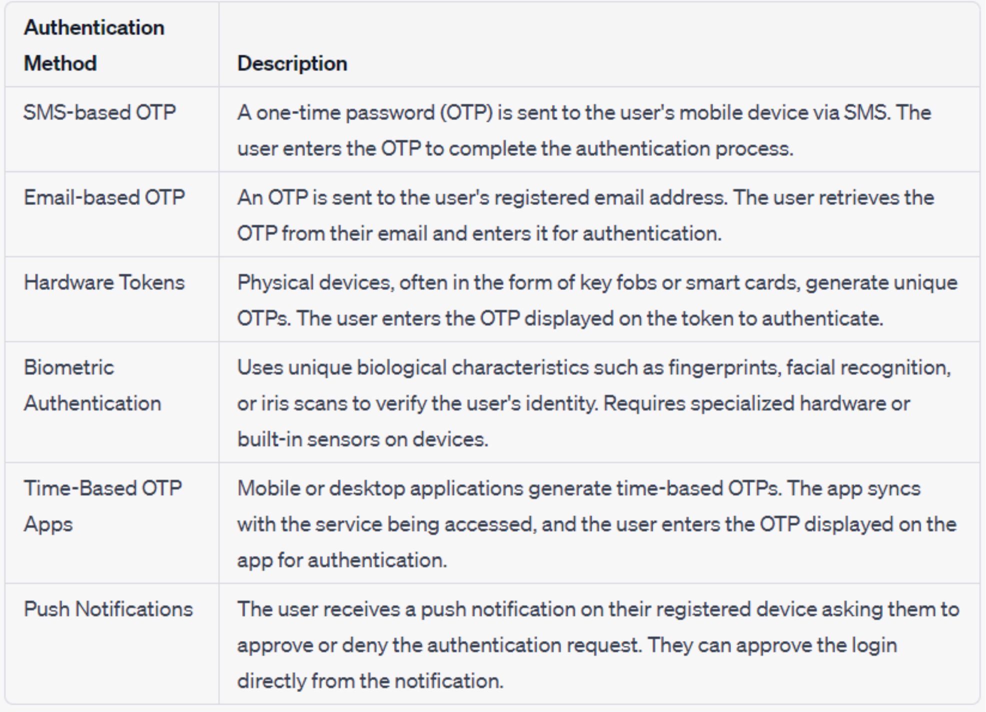
### 4. Testing the Proposed System

This step is the process of testing whether the programming code will work correctly with the conditions in our system or not. In this phase, we will fix bugs in order to produce a system with maximum performance.

### 5. Deploy and review

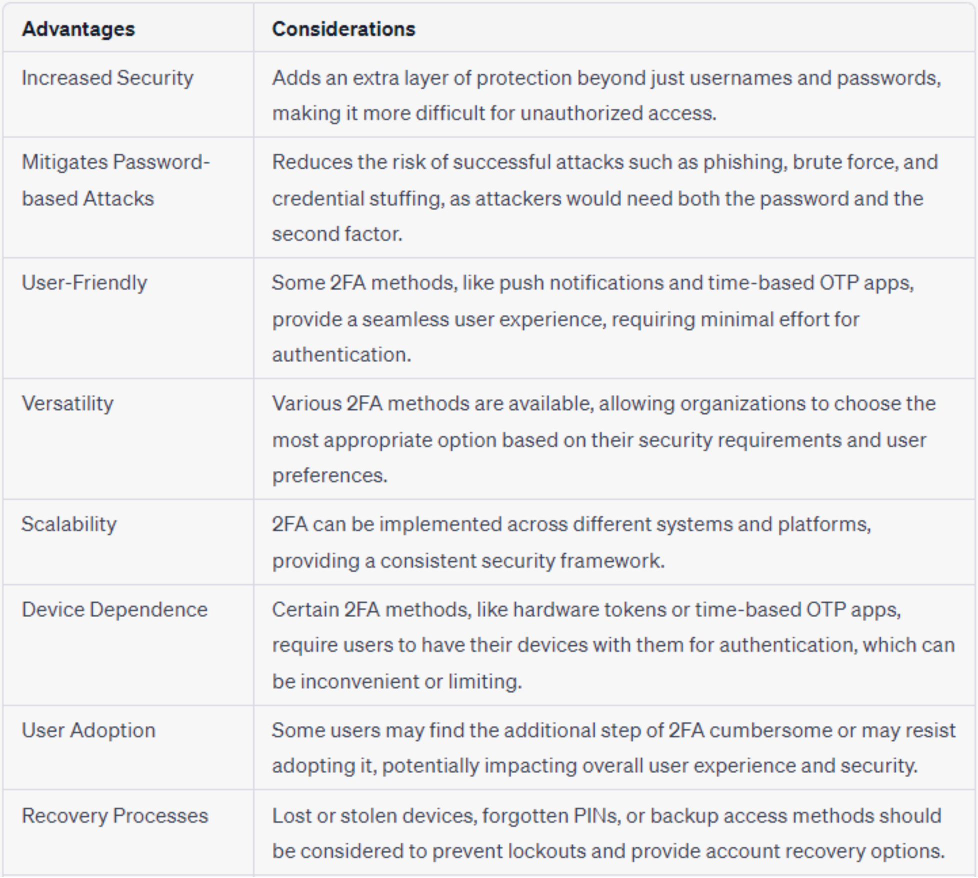
In this phase we deploy the development system to the leader and get reviews and feedbacks and comments and repeat the all cycles if needed.

## 3- RESULT



| Authentication Method | Description |
|---|---|
| SMS-based OTP | A one-time password (OTP) is sent to the user's mobile device via SMS. The user enters the OTP to complete the authentication process. |
| Email-based OTP | An OTP is sent to the user's registered email address. The user retrieves the OTP from their email and enters it for authentication. |
| Hardware Tokens | Physical devices, often in the form of key fobs or smart cards, generate unique OTPs. The user enters the OTP displayed on the token to authenticate. |
| Biometric Authentication | Uses unique biological characteristics such as fingerprints, facial recognition, or iris scans to verify the user's identity. Requires specialized hardware or built-in sensors on devices. |
| Time-Based OTP Apps | Mobile or desktop applications generate time-based OTPs. The app syncs with the service being accessed, and the user enters the OTP displayed on the app for authentication. |
| Push Notifications | The user receives a push notification on their registered device asking them to approve or deny the authentication request. They can approve the login directly from the notification. |

**Figure 3.1**



| Advantages | Considerations |
|---|---|
| Increased Security | Adds an extra layer of protection beyond just usernames and passwords, making it more difficult for unauthorized access. |
| Mitigates Password-based Attacks | Reduces the risk of successful attacks such as phishing, brute force, and credential stuffing, as attackers would need both the password and the second factor. |
| User-Friendly | Some 2FA methods, like push notifications and time-based OTP apps, provide a seamless user experience, requiring minimal effort for authentication. |
| Versatility | Various 2FA methods are available, allowing organizations to choose the most appropriate option based on their security requirements and user preferences. |
| Scalability | 2FA can be implemented across different systems and platforms, providing a consistent security framework. |
| Device Dependence | Certain 2FA methods, like hardware tokens or time-based OTP apps, require users to have their devices with them for authentication, which can be inconvenient or limiting. |
| User Adoption | Some users may find the additional step of 2FA cumbersome or may resist adopting it, potentially impacting overall user experience and security. |
| Recovery Processes | Lost or stolen devices, forgotten PINs, or backup access methods should be considered to prevent lockouts and provide account recovery options. |

**Figure 3.2**

## 4- DISCUSSION

Certainly! Two-factor authentication (2FA) apps are software applications that generate one-time passwords (OTPs) or receive push notifications to provide an additional layer of security during the authentication process. Here's a discussion about 2FA apps:

Functionality: 2FA apps generate time-based OTPs using a secret key shared between the app and the service being accessed. These OTPs typically change every 30 seconds, adding an extra layer of security beyond just a username and password.

Security Benefits: Using a 2FA app significantly enhances security because it requires physical possession of the device where the app is installed. This adds a second factor to the authentication process, making it much more difficult for unauthorized individuals to access an account even if they have the username and password.

Popular 2FA Apps: There are several well-known and widely used 2FA apps available:

Google Authenticator: Developed by Google, it is a popular choice supporting both time-based OTPs and push notifications.

Authy: Offers similar functionality to Google Authenticator but with the added benefit of cloud backup and multi-device synchronization.

Microsoft Authenticator: Microsoft's app that supports OTPs and push notifications and integrates well with Microsoft services.

Setup Process: To use a 2FA app, the user typically needs to enable 2FA on the respective service or website. This involves scanning a QR code provided by the service with the app, which establishes the link between the app and the account. Once set up, the app generates OTPs that must be entered during the authentication process.

Backup and Recovery: Some 2FA apps, like Authy, offer backup and recovery features. This allows users to restore their 2FA tokens when switching devices or if they lose access to their primary device.

Advantages and Considerations: Using a 2FA app provides an additional layer of security and is generally more secure than other 2FA methods like SMS-based OTPs. However, it's essential to consider the following factors:

Device Dependence: The app's functionality is tied to the device where it is installed, so users must have access to the device to generate OTPs.

Device Loss: If the device with the 2FA app is lost or stolen, account recovery processes should be in place to regain access to accounts.

Backup Options: Some apps offer backup features, which can be useful for device migration or when switching to a new device.

It's important to note that while 2FA apps are a secure option, there are alternative methods available, such as hardware tokens, SMS-based OTPs, or biometric factors. The choice of 2FA method depends on the level of security desired and the specific requirements of the service or application being accessed.

## 5- CONCLUSION

In conclusion, two-factor authentication (2FA) is a highly effective method for enhancing the security of online accounts and systems. By requiring users to provide two separate forms of identification, typically a password or PIN and a second factor such as a fingerprint, facial recognition, or a unique code sent to a mobile device, 2FA significantly reduces the risk of unauthorized access and data breaches.

The key advantage of 2FA lies in its ability to provide an additional layer of protection beyond traditional password-based authentication. Even if a hacker manages to obtain or crack a user's password, they would still need the second factor to gain access. This significantly increases the complexity of unauthorized access attempts, making it far more difficult for attackers to breach user accounts.

Furthermore, 2FA offers increased convenience compared to more traditional security measures such as one-time passwords sent via SMS. With the emergence of mobile authentication apps and hardware tokens, users can conveniently generate or receive the second factor on their own devices, eliminating the need for relying on external communication channels.

The widespread adoption of 2FA by major online platforms and services has demonstrated its effectiveness in preventing unauthorized access and protecting sensitive information. It has proven to be an essential tool in mitigating the risks associated with password-related vulnerabilities, such as weak passwords, password reuse, and phishing attacks.

However, it's important to note that no security measure is entirely foolproof, and 2FA is not without its limitations. Some potential challenges include the possibility of losing or damaging the second factor device, the risk of SIM card swapping or device theft for SMS-based authentication, and potential vulnerabilities in the implementation of the 2FA system itself.

To maximize the effectiveness of 2FA, it is crucial for users to select strong and unique passwords, regularly update their devices and software, and employ additional security measures such as biometric authentication where available. Service providers and developers must also stay vigilant in implementing robust 2FA systems and keeping up with evolving security best practices.

Overall, two-factor authentication is a powerful and necessary security measure in today's digital landscape. By adding an extra layer of protection, it significantly enhances the security of online accounts and systems, making it considerably more difficult for unauthorized individuals to gain access. While it is not without its challenges, when properly implemented and utilized in conjunction with other security practices, 2FA is an invaluable tool in safeguarding sensitive information and protecting against cyber threats.

## ACKNOWLEDGEMENT

We extend our sincere gratitude to Dr Alaa Zaghloul for granting us the exceptional opportunity to work on the remarkable project of developing a Construction online blood bank management system. Throughout this journey, we have acquired invaluable knowledge and skills that will greatly benefit our professional growth. We are profoundly grateful to Dr Alaa Zaghloul for his unwavering guidance, continuous supervision, and provision of essential project-related information. Moreover, we deeply appreciate his support during the entire project completion process.

Dr Alaa Zaghloul's constant guidance and willingness to share his vast knowledge have allowed us to comprehend the project and its intricacies in great depth, enabling us to successfully accomplish our assigned tasks within the designated timeframe. We also express our thanks and appreciation to our colleagues who actively contributed to the development of this project, as well as those individuals who willingly offered their assistance and expertise.

Once again, we extend our heartfelt thanks to Dr Alaa Zaghloul for his invaluable support and the opportunity to be part of this rewarding project.

## 6- REFERENCE

[1] "Two-Factor Authentication" on Wikipedia:

- Link: https://en.wikipedia.org/wiki/Two-factor_authentication

[2] "Two-Factor Authentication (2FA)" on OWASP (Open Web Application Security Project):

- Link: https://owasp.org/www-community/Two-Factor_Authentication_(2FA)

[3] "What is Two-Factor Authentication (2FA) and How Does It Work?" by Duo Security:

- Link: https://duo.com/learn/what-is-two-factor-authentication