IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

X-Facto: 2FA Authentication Application

Aditya Nikose
Department of Computer Engineering
Vidyalankar Institute of Technology
Mumbai, India
aditya.nikose@vit.edu.in

Saumya Singh
Department of Computer Engineering
Vidyalankar Institute of Technology
Mumbai, India
Saumya.singh@vit.edu.in

Roshan Karkera
Department of Computer Engineering
Vidyalankar Institute of Technology
Mumbai, India
Roshan.karkera@vit.edu.in

***Abstract*—The access control system is an important security feature to protect assets from being accessed illegally. One of the security techniques for access control is the use of biometrics.[1] Two-factor authentication techniques using mobile devices are proposed. The method allows biometric features inseparable from the owner of the device, characterized by the features of his fingerprint. Two-factor authentication provides a significant increase in security. No longer will an unsecured password provide enough information to a hacker to allow a breach in security. The password or pin number must be used in conjunction with the use of tokens, smart cards, or even biometrics.**

Keywords—User Authentication, Biometric Authentication, Two-factor authentication, Smartphone, TOTP

I. INTRODUCTION

Historically, the use of PINs, passwords, names, numbers, social security, and tokens has been widely used to verify that someone is recognized by the system. In its implementation, many passwords use the system to identify the correct password without knowing whether the password is used by the correct person.[2] Different from the above problems, biometrics can offer prospects that closely link the authenticity of an individual person. The biometric system establishes a probabilistic assessment of a match which shows that the subject is the same as who the reference is stored.

Nowadays, many organizations utilize log-in features to allow users to access protected information. For a long time, passwords and usernames have been the standard for achieving this. The problem with this is that people tend to use weak passwords and often the same password for multiple domains. Shared passwords between multiple domains, especially weak passwords, present security risks, since an attacker could exploit this to gain unauthorized access to one or several of users' accounts.

One of the biometric factors that can be implemented is fingerprint recognition. It is one of the patterns approaches for personal identification purposes in addition to other biometric approaches such as facial recognition, signature, retina of the eye, and so on.[3] The fingerprint is one part of the human body that has a unique characteristic that can identify a person. Everyone has differences starting from the form of patterns and their own characteristics on the finger.

As reported, mobile devices sales in 2021 amounted to 11% compared with the previous year, including an annual increase of 11.3% for modern smartphones. According to online research, the sales market volume of the devices will reach 1351.8 billion units by 2025, with an average annual growth rate of 11.2%. Such great interest in mobile devices (tablets, smartphones) is caused by their capabilities. Users of modern mobile devices can communicate with people from different parts of the world, access bank accounts, use remote storage with valuable information and various online accounts, etc. However, it is followed by security issues. The most serious risk is unauthorized access to personal data.

Any data protection system is based on identification and authentication. At present time, the most common authentication method is a password-based authentication mechanism. For successful authorization, a user must reproduce the combination of his unique identifier (usually a phone number or email address) and password. With the increase in account quantity, computer users may have issues with remembering a large number of identities. So that users of such systems prefer saving the credentials in a browser or a client application, greatly reducing the effectiveness of password-based protection mechanisms since access to user accounts is available to any person who has received the user's device with saved credentials. An affordable solution to the problem is a two-factor authentication system using a single-use SMS password. Currently, two-factor authentication systems are widely used to provide access to online banking, making purchases via the Internet, social networks, and so on.[3]

But it should be considered that modern mobile devices have a lot of functions, such as Internet access and the ability to install third-party mobile applications. Thus, often mobile devices are used for working through the Internet, as the result of which two-factor authentication is ineffective since with getting access to the mobile device an attacker also sees incoming messages with single-use SMS-passwords. In the case of alienation of such mobile devices from the user, an authentication procedure can be performed without the warning of the device's owner.[3]

So, currently, there is a need for the implementation of widely available biometric authentication technologies protected from identifier alienation from the owner (user) and invulnerable to identifier alienation from the owner (user). One of the biometric authentication methods, available for deployment on many modern mobile devices, is user authentication technology using handwriting dynamics of a signature or fixed (handwritten) password. This technology is related to dynamic biometrics. Previously, this method required purchasing additional equipment – a graphical tablet (digitizer) with light or inductive pen. Last year, most mobile devices are equipped with input touch-screens that can be used instead of digitizers. At the end of 2012, Scientific-Technical Center mKASIB released a beta-version of cloud service which implements the user authentication technology using password writing dynamics, as a service. Dynamics means the set of the signature's form, writing speed, and pen pressure (the last one is obtained from the devices having an inductive screen and stylus). Signature writing dynamics are unique for every person and can be comparable with fingerprints. In the case of a graphic image of the signature being quite similar to the reference sample, but written by another person, the system does not authenticate the person because of the differences between the signature dynamic characteristics. The matter of the signature and etalon sample comparison is to build hypotheses on the percent of similarity of test sample and etalon sample. Bayesian networks are used for the comparison of biometric images with the reference template, in particular, an algorithm of consistent application of the modified Bayes hypothesis formula, which gives quite good results on the pattern recognition in the space of uninformative signs.[3]

II. LITERATURE REVIEW

A. *Related Work*

In this section, we analyze the two-factor authentication method and biometric authentication method.

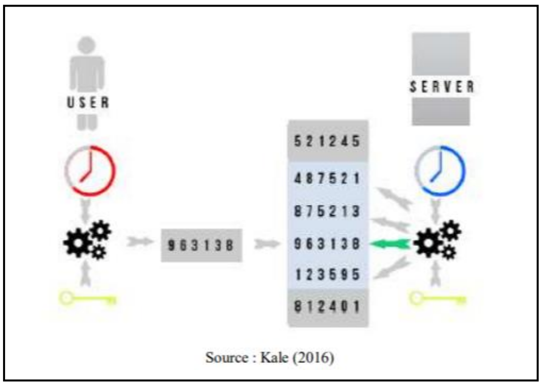
B. *Two-factor Authentication*

Two-factor authentication is not a new concept. It is a term used to describe any authentication mechanism where more than one factor is required to authenticate a user. It has been used throughout history by having a known person utter a password. Traditional authentication schemes used username and password pairs to authenticate users. This provides minimal security because many user passwords are very easy to guess. Therefore, studies in two-factor authentication are increasing. Using two factors, as opposed to one factor, generally delivers a higher level of authentication assurance. Two-factor authentication typically is a signing-on process, where a person proves his or her identity with two of the three methods: "something you know" (e.g., password or PIN), "something you have" (e.g., smartcard or token), or "something you are" (e.g., fingerprint or iris scan). Using more than one factor is sometimes called "strong authentication". However, "strong authentication" and "multi-factor authentication" are fundamentally different processes.[1][4]

C. *Biometrics*

It is one of the competing technologies for implementing two-factor authentication. Biometrics uses something you are, as an authentication factor, instead of the something you have mechanism utilized in traditional two-factor authentication. Many studies have proposed biometric-based authentication schemes. In 2010, Li and Hwang proposed an efficient biometric-based remote user authentication scheme using smart cards. This scheme uses simple hash functions and nonce to make the authentication scheme efficient. It uses the random nonce, rather than a synchronized clock, thus it is very efficient in computational cost. However, this scheme does not provide proper authentication and cannot resist man-in-the-middle attacks. To solve the drawback of Liet al. (2011) scheme proposed an improved biometrics-based remote user authentication scheme that removes the weaknesses and supports session key agreement. This scheme uses a password with a random nonce to provide proper authentication in the login and authentication phase. However, this scheme again fails to provide it, because there is no verification on the user's entered password after successful verification of the biometric template. Das (2011) proved this drawback on paper.[1][6]

D. *TOTP*



Source : Kale (2016)

Fig. 1. TOTP generation process

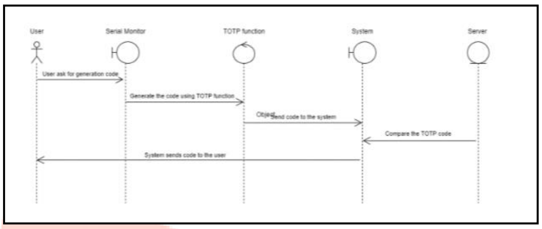

User
Serial Monitor
TOTP function
System
Server
User ask for generation code
Generate the code using TOTP function
Object
Send code to the system
Compare the TOTP code
System sends code to the user

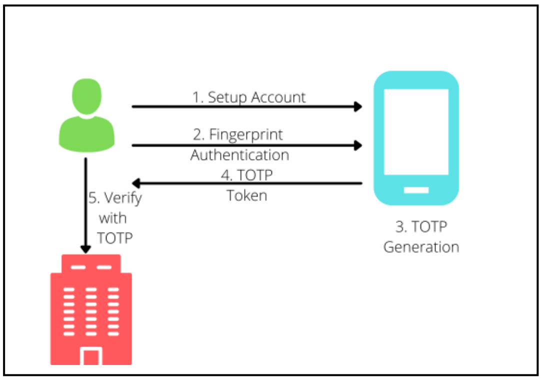
Fig. 2. Sequence Diagram of TOTP generation process

TOTP (Time-Based One-Time Password) is an algorithm that applies hash-based message authentication (HMAC). This algorithm is a specific type of message authentication code (MAC) that involves a hash cryptographic function in a secret cryptographic key combination. The strength of HMAC cryptography depends on the cryptographic strength of the underlying hash function, its hash output size, and key quality measures. The TOTP used in this study produced a temporary cipher key that changes with time as shown by the process in Fig. 1 and Fig. 2 is shown about generation code using TOTP and sending the code to the user. The time required to generate a new cipher key is 30 seconds so it is difficult to crack. The hash function used in TOTP is SHA-1. [2]

III. PROPOSED WORK

Prerequisites - XFacto mobile application should be installed on the user's mobile phone.

The workflow of the system goes as follows:



A. Setup Account

The procedure will be as follows: The user wishes to protect an account with 2fa, for this the user will navigate and click the add account button, after this the user will enter the details such as the name of the organizational account that will be protected by 2fa.

This will also be the step where a pre-shared key will be generated for that particular account. This pre-shared key will play an important role in the generation of TOTP. This preshared key will be generated by scanning a QR code, This QR code will be provided by the organization itself. The user will just have to scan this QR code to set up the account that needs protection.

B. Fingerprint Authentication

Once the Account setup has been done by the user, the user can be rest assured about the 2fa, now whenever the user logs into this account the user needs to establish his identity yet again using xfacto hence 2fa.

The user will be prompted to click the authenticate button in front of the account that he set up on xfacto, using local fingerprint authentication the totp generation process will start.

C. TOTP Generation and verification

OTP could increase the security of the proposed model by incorporating volatile passwords. The change from static passwords would make it very unlikely to make any successful password related attacks as they would keep changing. It is very important that the implementation of OTP is text-book implemented, if not it could potentially provide lesser security. Theoretically the attacker would either have to resort to stealing the phone or get a hold of the OTP algorithm.

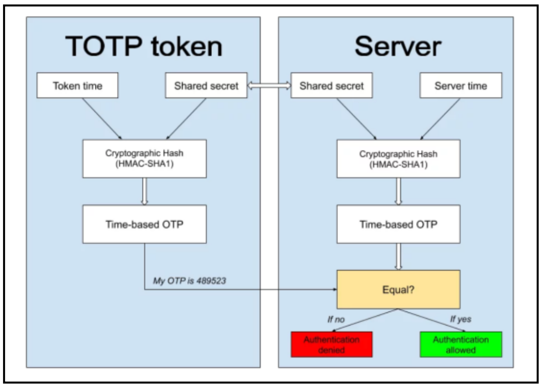
Choosing between HOTP and TOTP is a matter of cost, theoretically TOTP is the best choice since a password can only be valid within a fixed time frame, whereas HOTP could be valid for a very long time. However, TOTP requires that server and application must be in sync for the password generation to work.

A user wants to log into a TOTP 2FA protected application or website. For the OTP authentication to run, the user and the TOTP server need to initially share a static parameter (a secret key).

When the client logs into the protected website, they have to confirm they possess the secret key. So their TOTP token merges the seed and the current timestep and generates a HASH value by running a predetermined HASH function. This value essentially is the OTP code the user sees on the token.

Since the secret key, the HASH function, and the timestep are the same for both parties, the server makes the same computation as the user's OTP generator.

The user enters the OTP and if it is identical to the server's value, the access is granted. If the results of the calculations aren't identical, the access is, naturally, denied.



IV. Implementation and Analysis

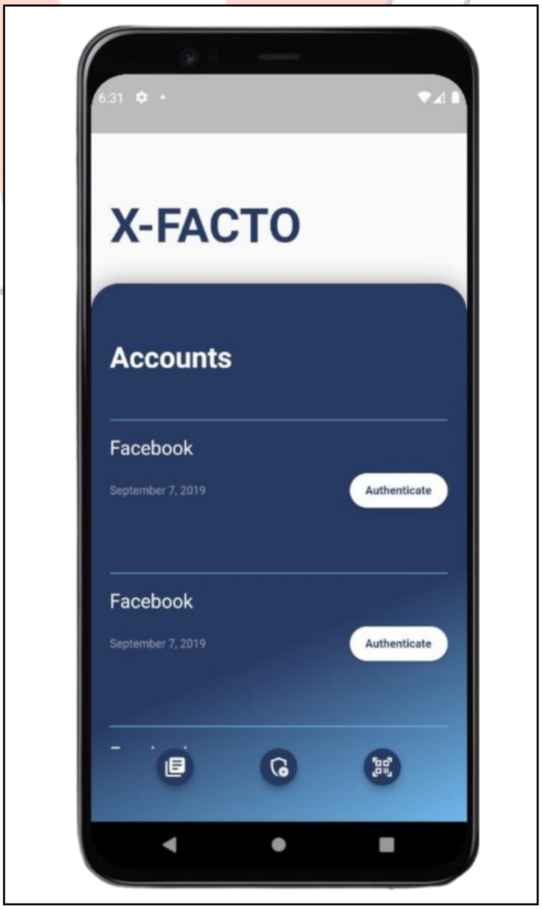
X-Facto is a mobile application built using flutter, we will be using the local authenticated dart library which will be used to authenticate users using his/her fingerprint that is stored locally on his device.

Flutter is faster than many other application development frameworks. With its "hot reload" feature, you can experiment, build UIs, add/remove features, test and fix bugs faster. Thus reducing the overall app development time.

A. Homepage of the application

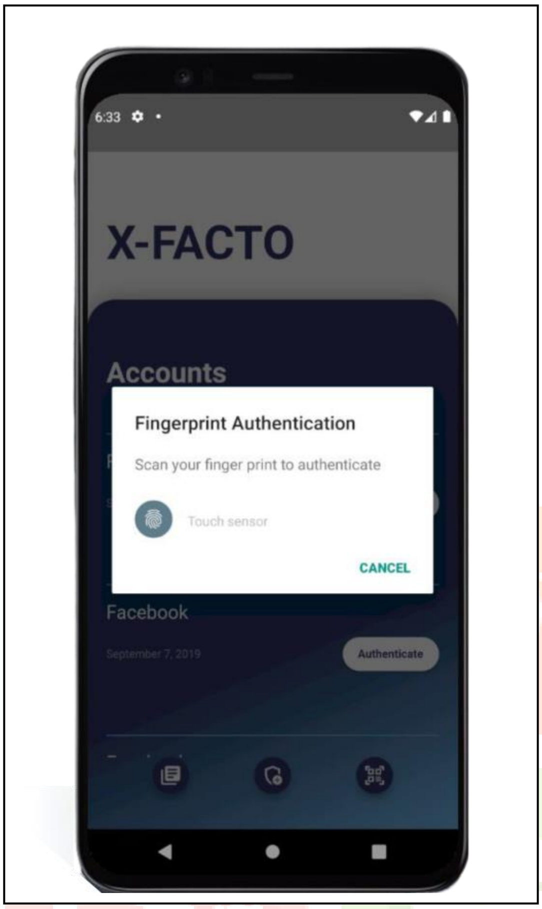
Let's have a look -

When the user launches Xfacto, and after setting up the account, user can expect a screen as shown in the figure below.



B. Authenticate

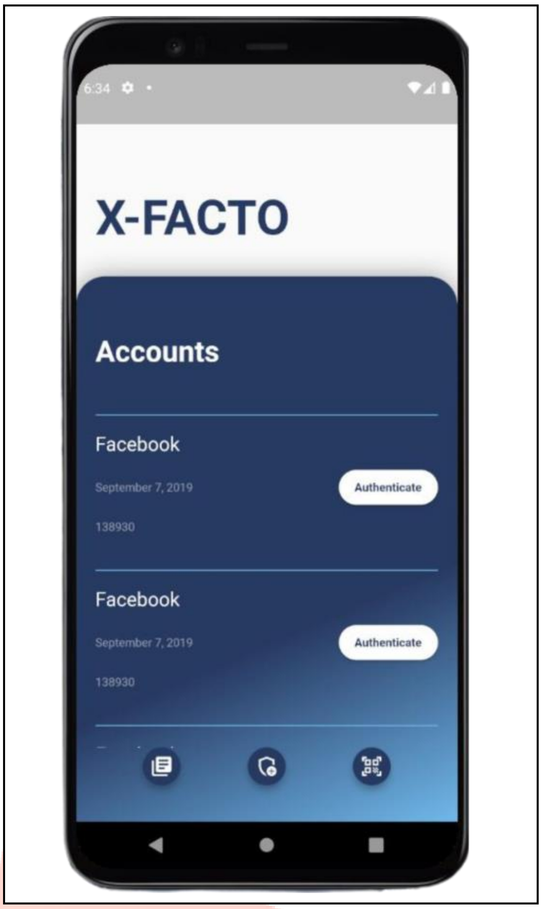
User can now click on the authenticate button for the authentication process, once he clicks the authenticate button a dialogue box appears as shown in the image below. The user has to provide his biometric identity i.e. his fingerprint to generate a TOTP.


Fingerprint Authentication

Scan your finger print to authenticate

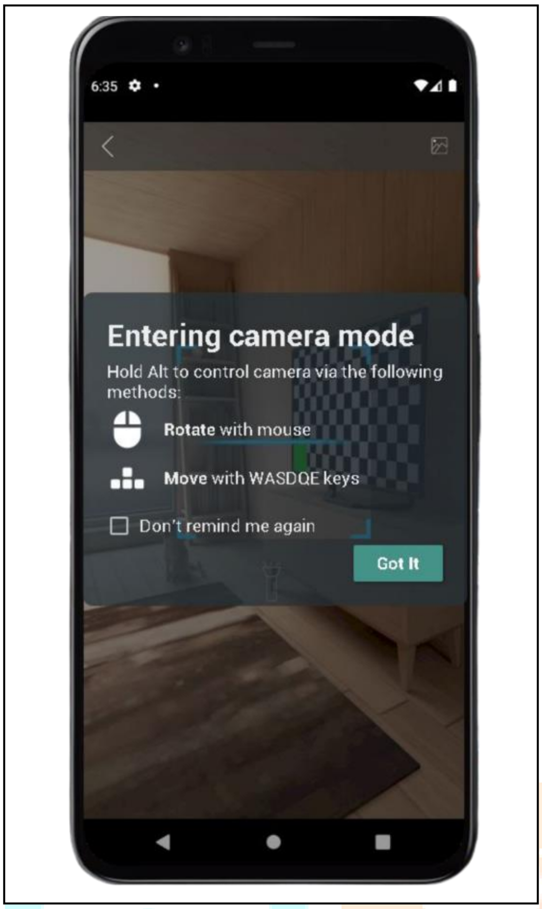
C. TOTP generation

Once the user provides his valid fingerprint the app generates a TOTP as seen in the image below.
The user can now simply use this TOTP to complete the authentication process



TOTP - 138930

It is important that each and every user gets a unique TOTP generated at a given point of time. No database backend is being used to hold any critical data of the user. To separate the different identities, we will be using a secret code which can be generated and stored in the app for that particular device. This secret code will be generated by scanning of the qr code which will be unique for all users and will be provided by the organization. In the fig below we can see the QR Scanner screen



Entering camera mode

Hold Alt to control camera via the following methods:

Rotate with mouse

Move with WASDQE keys

□ Don't remind me again

V. Result and Discussion

Security of secret Key

The proposed system has two pieces of secret information one is the qr code and the other one is secret code generated from this qr code. The attacker can't generate a QR code for a particular user as this is generated by the organization for each specific user. The attacker also cannot generate the secret code which is a base32 string.

Stolen phone

Lost phone does not present an immediate risk since fingerprint authentication is required.

Replay attack

An attacker cannot possibly intercept the password exchange between the application and server to get hold of sensitive information. As there is only one thing which is being communicated i.e if the authentication is successful or not. Replay attack can be prevented using session id

Brute-force attack

The proposed model is not susceptible to a brute-force attack

Web site forgery

Since the application handles the authentication process almost exclusively, the security risks involving the user and browser are heavily mitigated.

Dictionary attack

The proposed model is not susceptible to a dictionary attack.

Interaction	*Existing System*	*Proposed Model*
Enter Credentials	*Yes*	*No*
Enter TOTP	*yes*	*Yes*
Fingerprint	*No*	*Yes*

VI. Conclusion

The project X-FACTO will essentially provide an additional layer of security to the user and eliminate the risk of brute forcing attack and dictionary attack. It will help users and organizations to be more aware whenever an unauthorized user tries to gain access. The fingerprint based 2FA will grant access to only that person who is authorized to view or manipulate the information. It will successfully remove the need for changing password every 1 month for security purposes as there will always be a second layer protecting the user's information.

References

[1] How Electronic Access Control Systems Work, Thomas L. Norman CPP/PSP, in Electronic Access Control (Second Edition), 2017

[2] Eric Knipp, ... Edgar Danielyan Technical Editor, in Managing Cisco Network Security (Second Edition), 2002

[3] Integrated Identification Technology, Clifton L. Smith, David J. Brooks, in Security Science, 2013

[4] Two Way Mobile Authentication System, Harish Dinne and Karthik Mandava, in Master Thesis Electrical Engineering, 2010

[5] A Theoretical Proposal of Two-Factor Authentication in Smartphones, Oskar Persson and Erik Wermelin, Bachelor Thesis in Computer Science, May 2017

[6] Context-Aware Multifactor Authentication Survey, Emin Huseynov, Jean-Marc Seigneur, in Computer and Information Security Handbook (Third Edition), 2017

[7] An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications, Chun-Ta Li and Min-Shiang Hwang, 2009

[8] Improvement of Li-Hwang's biometrics-based remote user authentication scheme using smart cards, 2011

[9] PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables, 2020

[10] Two-factor authentication for voice assistance in digital banking using public cloud services, London Metropolitan University, 2020