IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

Study of Multi-Factor Authentication

Divya Dinesh Mhatre[1] and Sweta Nag[2]
Students, Department of MCA[1,2]
Sterling Institute of Management Studies Nerul, Navi Mumbai, Maharashtra, India

Abstract: *One of the most effective ways to ensure secure authentication is to use digital multifactor authentication. The Multi-Factor Authentication method was implemented after many experiments to protect the data by raising its security level to the next level with additional authentication. Various authentication factors have been introduced, which are then linked to direct access. All aspects of modern culture are now rapidly expanding as a result of digitalization. Verification is one of the most powerful empowering factors in breaking the pattern. It includes online payments, organization, access rights management, and other aspects of living in a hyper-connected world. The growing interest in high-security applications has sparked interest in obtaining sensitive information through the use of passwords, tokens, and other methods. Modernized mystery key gathering projects discover quick, obvious, and easy-to-guess passwords such as names and ages easily. Malware is a persistent threat to security and protection, both in terms of quantity and consistency. As data becomes more available, hacking, secret key breaking, and online misrepresentation become less effective. The multi-factor confirmation proposition ensures a higher level of safety by increasing the single verification factor.*

Keywords: Authentication, Multi-Factor Authentication, Sensors, Cryptography, Face recognition, One Time Password (OTP), Password, Biometrics, Token, Verification, Data Protection

I. INTRODUCTION

Authentication is critical, especially in online services. There are several methods for authenticating users. These range from simple systems like a username and password combination to complex systems like biometric and/or one-time usage based variable tokens.

1.1 Authentication

Authentication is the use of one or extra mechanisms to prove our identification. The use of one or more mechanisms to prove our identity is known as authentication.[1]

II. HOW AUTHENTICATION WORK

The first step is to enter your login information on a login page or in the username and password bar. The following step is to validate your login information. When the server you're attempting to access decrypts the personalized information it receives, the authentication process begins. Finally, the computer either approves or rejects your authentication request.[2]

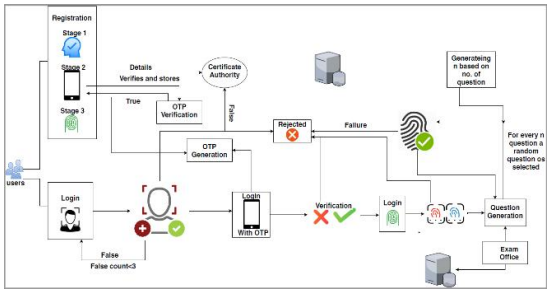


Fig.1Working of authentication

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

III. WHY IS AUTHENTICATION IMPORTANT?

Cybercriminals spend their days preying on unsuspecting victims. To stay safe as an active online user, you must protect your devices from unauthorized access.

User authentication is effective in reducing cyber threats to their most basic form. Attackers' antics are only credible if they gain access to your network. The authentication acts as a barrier that keeps them out. They can't pull it down as long as it's strong.

User authentication protects the confidentiality, builds trust, and ensures privacy.[2]

IV. TYPE OF AUTHENTICATION

	Single Factor Authentication	Two Factor Authentication	Multi Factor Authentication
Definition	Single-factor authentication is the simplest form of authentication methods. With SFA, a person matches one credential(password) to verify himself or herself online[3]	Two-factor authentication uses the same password/username combination, but with the addition of being asked to verify who a person is by using something only he or she owns, such as a mobile device. Simply put, it uses two factors to confirm an identity.[3]	Multi-factor authentication combines three factors: something you know, something you have, and something you are. MFA[3] is a subset of 2FA.[3]
Why is it used	The process of single factor authentication is much simpler and faster.[4]	Two-factor authentication provides a higher level of security than single-factor authentication (SFA)[4].	It has more security layers than 2FA[4].
Pros	Single FA is simple because you only have to go through one process[6].	The main advantage of such two-factor authentication software is its ability to be used in the absence of cellular coverage or Internet access[7].	To use a stolen MF software / hardware authenticator, an attacker still requires the second factor[8].
Cons	It is capable of leaking passwords. A keylogger or screen capture can be used to steal the password[6].	If the device is factory reset or lost, or the authenticator application is accidentally deleted, the token is lost and recovering it is difficult[7].	The second factor is on the same device as the first. When the second factor is verified locally, such as with an OTP software generator on a smartphone, both the second factor and the secret key used to generate the OTP may be compromised at the same time[8].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

V. LITERATURE REVIEW

To better comprehend the elements at work with authentication, it's far critical to first comprehend what authentication is. Authentication and the various measures of authentication are used to confirm that a specific consumer or manner is who they claim to be. It really is that simple. There are four well-known methods for authenticating customers [9]:

- **Something you Know:** This is the most basic type of authentication with which most customers are familiar. This well-known is typically provided as a username or password that the consumer understands best.
- **Something you own:** This type of authentication is represented by the consumer having ownership of a physical entity or tool. This can be represented as a physical token consisting of the consumer's cellphone or other media device producing a brief and, on occasion, single use authentication code [9].
- **Something You Are:** A biometric signature, which includes a fingerprint, retina scan, or facial recognition, represents this type of authentication. When done correctly, this is usually visible as one of the most powerful types of authentication.
- **Someplace you are**: This type of authentication corresponds to the location of a consumer or method, and in response offers or denies access to sources accordingly. This well-known can be accomplished by employing a large number of IP addresses or geographic area points [9].

The efficient use of biometrics and other authentication methods ensures the implementation of a future market standard of a three-factor authentication approach. Dependability breeds confidence, and confidence breeds efficiency. The increased dependability of a more secure platform with three-factor authentication is difficult to dismiss. With additional research, the software could be expanded to allow users to create their own accounts and save credentials and biometric reference tags in each user's account [9].

Multi Factor authentication (MFA) is a secure tool type that uses multiple forms of authentication to confirm the legitimacy of a transaction. In contrast, single component authentication (SFA) requires only a person ID and password. In two-factor authentication, the person provides two forms of identification, one of which is normally a physical token, such as a card, and the opposite of which is normally something memorized, such as a security code. Other authentication strategies that may be used in MFA include finger scanning, iris reputation, facial reputation, and voice ID [10,11,12, and 13].

The proposed system is an MFA scheme that benefits from various authentication schemes. Users have complete control over whether or not the 3-D password is entirely recall, biometrics, recognition, or token based, or a combination of schemes or more. This type of option is critical because users are unique and have different requirements. As a result, in order to ensure high user acceptability, the user's freedom of choice is critical.

VI. PROBLEM DEFINITION

The risk of critical data breaches grows in lockstep with the rate of digitization. As a result, robust systems capable of preventing or limiting the spread of stolen personal data are required. This could be accomplished by using a combination of multifactor authentication to strengthen a user's identity. Most authentication systems have varying requirements, both in terms of security and the complexity of the user authentication process. As a result, continuous authentication may be an effective way to provide additional security while remaining undetected by the user. As smartphones and wearable technology become more widely available, new authentication methods that are both easier to use and more secure than passwords are being proposed.

There are numerous methods for gathering user identifying features on smartphones because they contain a range of sensors. Apple, for example, uses both fingerprint and facial recognition as methods of authentication. [14,15]

VII. OBJECTIVE

The objective is to maintain a greater level of user authentication security. Users will be given access to set passwords at will. Text encryption, such as a pass phrase, a PIN or pattern-based password, and multi-factor authentication are all included. This way, whether you break the first or second level, or it's impossible to postpone a third, the bot or anybody else will have a harder time cracking password. As a result, as technology advances, new and unconventional methods are employed. The major goal of the multi-factor authentication security strategy is to provide a unique arcane lesson on how to use a 3-level authentication such as OTP as a password to make the system incredibly safe.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

VIII. RESEARCH METHODOLOGY

Every day, corporations, government agencies, and other organizations spend a lot of money on computer memory to preserve their data. Although online password guessing has been known since the dawn of the internet, there has been little teaching on how to avoid it. This paper examines multi-factor authentication in the context of a safe authentication system. When setting a password, for example, the user can choose three click points using a PIN or pattern. After evaluating the checkpoint, the user must log in again and confirm the next step of the login procedure, which is the delivery of the Soft Token to the phone number.

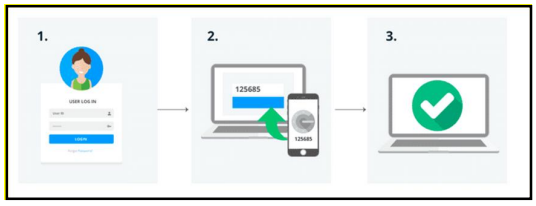


Fig. 2 How Multi-factor works[16]

As a result, this feature encourages users to select Image and click difficult-to-guess points. Remote login is presently full and growing due to brute force and dictionary password attacks. Despite the threat of such an attack, allowing legitimate users to log in quickly is a critical issue. Automatic Turing Check is being developed as an effective, simple-to-use solution - using the default login detection method charges users automatically.

8.1 Shamir's Secret Sharing Scheme

Shamir's Secret Sharing scheme[16] can be used to divide an integer into s to n shares. If a certain number of shares, t, are available, the secret integer, s, can be successfully modernized. The Dealing algorithm is used to split the integer, and the reconstruction algorithm is used to modernize the secret.

The Dealing algorithm is given in Fig. 3 and Reconstruction algorithm in Fig. 4

Algorithm 1 Shamir's Secret Sharing Scheme: Dealing Algorithm

Input: Number of shares n, Threshold value t, a prime number q and Secret integer $s \in \mathbb{Z}_q$

Output: A list of n shares, $\zeta = \{s_i\}$ *where* $1 \leq i \leq n$

Randomly choose $t-1$ random integers $a_1, a_2, a_3 \ldots a_{t-1}$

$a_0 \leftarrow s$

Build the polynomial

$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$

for $i \leftarrow 1$ *to* n **do**

$s_i \leftarrow (i, f(i) \mod q)$

end for

return ζ

Fig. 3 Proposed Dealing algorithm

Algorithm 2 Shamir's Secret Sharing Scheme: Reconstruction Algorithm

Input: A list of shares, $S = (x_i, y_i) \forall i > 0$

Output: The reconstructed value, s'

for *each* $j \mid (x_j, y_j) \in S$ **do**

$$\ell_{j,0,S} \leftarrow \prod_{\substack{(x_m, y_m) \in S \\ m \neq j}} \frac{-x_m}{x_j - x_m} (mod\ q)$$

end for

$$s' = \sum_{(x_j, y_j) \in S} y_j \ell_{j,0,S} (mod\ q)$$

return s'

Fig. 4 Proposed Reconstruction algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

Multi-factor authentication using fingerprints and user-specific random projection

The proposed multi-factor authentication method [18] is divided into two phases: enrolment and verification. The fingerprint and the secret key are required inputs during the enrollment phase (user-specific PRN). The PRN is used to generate a user-specific random matrix mxm RR, which is then stored on a smartcard. A fixed length vector n Rx is extracted from the fingerprint and then projected onto a random subspace using the user-specific R, resulting in a revocable and privacy-preserving biometric template n Rt, which is then stored in the template database.

Random projection is a tool for reducing dimensionality. It can also be used to create biometric templates that are revocable while maintaining privacy.

During the verification phase, the user asserts his or her identity and provides a fingerprint and a PRN. The same template generation action used in the enrolment phase is then used to generate a template n' Rt. The similarity between t and 't is calculated. Between two vectors, the Euclidean range was used. If the Euclidean range between their query and enrolled templates is less than a predetermined threshold, the users are verified to be who they claim to be.

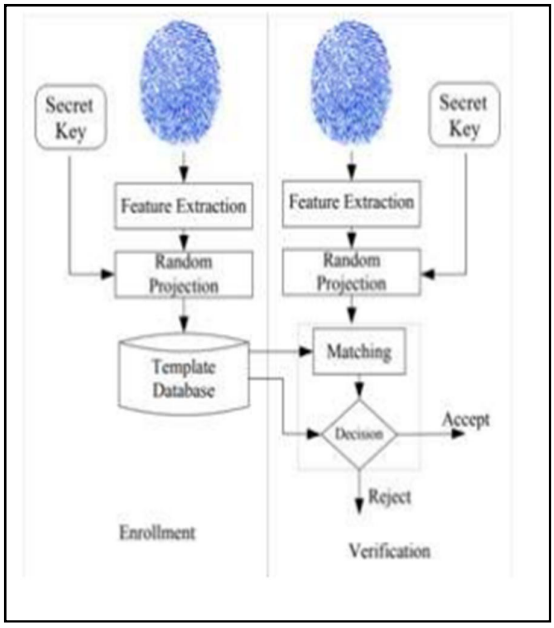


Fig . 5 Proposed Multi Factor Authentication System

IX. ANALYSIS & FINDINGS

A survey was administered to the group of people with the goal of learning about authentication as well as comparing and selecting various schemes and approaches. The survey form was filled out by 301 respondents in total and we received valid responses.

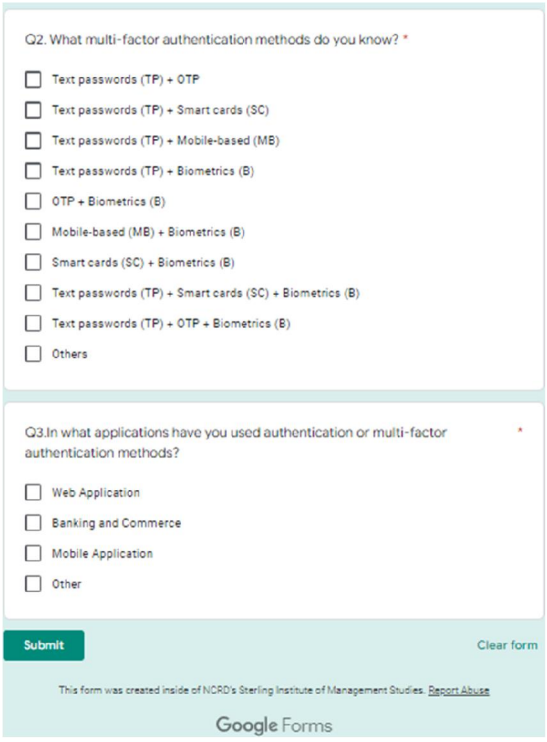
The respondents were asked three primary questions, the contents of which can be described as follows:

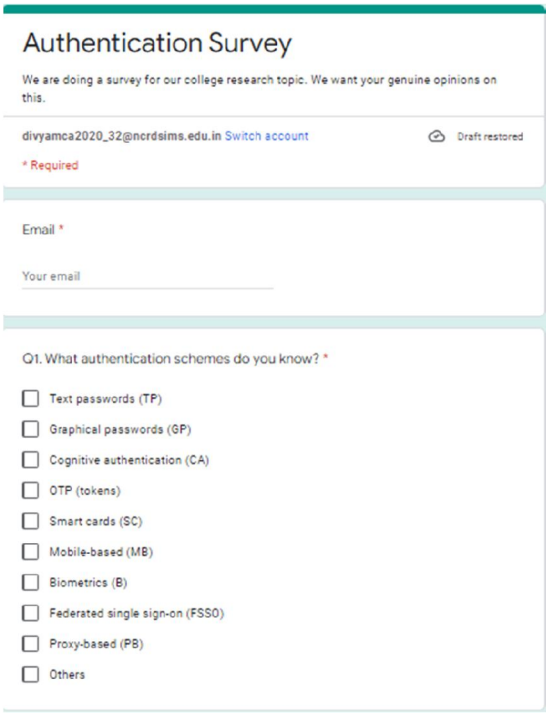
Q1. What authentication schemes do you know?

Q2. What multifactor authentication methods do you know?

Q3. In what applications have you used authentication or multi-factor authentication methods?

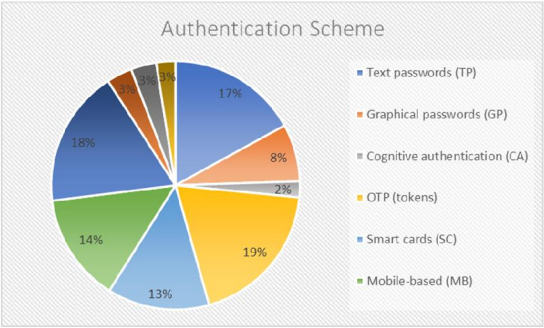
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252





9.1 Authentication Schemes known by the Respondents

For this question, respondents were asked to select the authentication schemes they were familiar with from a list. Text passwords, one-time passwords (OTP, tokens), and mobile-based authentication were the most well-known schemes. This question was answered by all respondents. The full results of this question are shown in Table 2, which shows the number of survey respondents who are familiar with each authentication scheme.



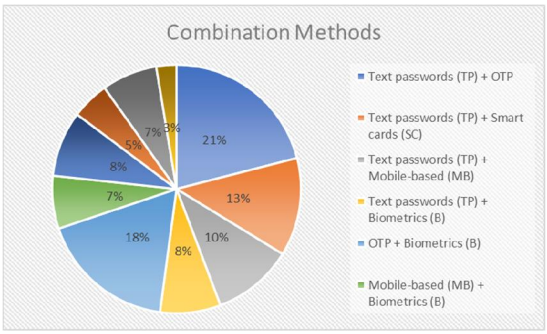
Authentication Scheme	Survey respondents
Text passwords (TP)	41
Graphical passwords (GP)	18
Cognitive authentication (CA)	5
OTP (tokens)	46
Smart cards (SC)	32
Mobile-based (MB)	34
Biometrics (B)	43
Federated single sign-on (FSSO)	8
Proxy-based (PB)	8
Others	6
Total	241

Table 1: Number of respondents that know each authentication scheme.

9.2 Multifactor Authentication Methods known by the Respondents

For the second question, respondents were given a brief explanation of multifactor authentication. Following that, they were asked what multifactor authentication methods they were familiar with. The most well-known of these was the combination of text passwords and OTP. This question was answered by 305 survey participants. The complete results of this question can be found in Table 3, which shows the number of survey respondents who are familiar with each multifactor authentication method.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

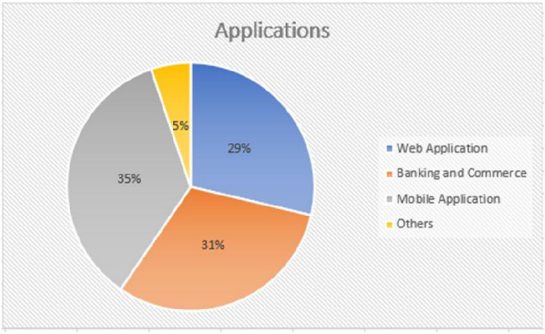


Combination	Method	Method2
Knowledge + possession	Text passwords (TP) + OTP	64
Knowledge + possession	Text passwords (TP) + Smart cards (SC)	39
Knowledge + possession	Text passwords (TP) + Mobile-based (MB)	32
Knowledge + possession	Text passwords (TP) + Biometrics (B)	24
Knowledge + possession	OTP + Biometrics (B)	54
Knowledge + possession	Mobile-based (MB) + Biometrics (B)	21
Knowledge + possession	Smart cards (SC) + Biometrics (B)	26
Knowledge + possession	Text passwords (TP) + Smart cards (SC) + Biometrics (B)	15
Knowledge + possession	Text passwords (TP) + OTP + Biometrics (B)	22
Knowledge + possession	Others	8
Total		305

Table 2: Number of respondents that know each authentication method.

9.3 Authentication Schemes and Methods used in Application by the Respondents

The respondents were then asked which authentication methods they had used in the application. The majority of applications were either mobile applications or banking and commerce applications. This question was answered by 136 survey respondents. The complete results of this question can be seen in the graphs of Figures 6, which show the authentication schemes and methods that were used, as well as the contexts of the applications that were used.



Applications	Survey respondents
Web Application	39
Banking and Commerce	42
Mobile Application	48
Others	7
Total	136

Table 3: Authentication schemes and methods used by the respondents.

X. LIMITATIONS

Multi-factor authentication takes more time Not only does having to enter two or more types of authentications add time to a process, but the installation itself can be tedious. Good multi-factor authentication should be programmed for both internal and external vendors, and getting everyone installed with the right access and tools does not occur overnight.

XI. CONCLUSION

Regardless of the issues with some authentication methods, it is clear that using multi-factor authentication in some form or another is far more secure than simply using a username and password. With users becoming more aware of security issues and the importance of protecting their online data, one of the first steps they should take to improve the security of their accounts is to enable multi-factor authentication.

REFERENCES

[1]http://hdl.handle.net/10603/341652
[2]https://www.makeuseof.com/
[3]https://www.centrify.com/blog/sfa-mfa-difference/#:~:text=Single%2Dfactor%20authentication%20is%20the,this%20type%20of%20authentication%20method.
[4]https://www.techtarget.com/searchsecurity/definition/two-factor-authentication
[5]https://www.centrify.com/blog/sfa-mfa-difference/
[6]https://zappedia.com/single-factor-authentication/

[7]https://www.protectimus.com/blog/two-factor-authentication-types-and-methods
[8]https://www.getidee.com/blog/mfa-vs-2fa
[9]William Kennedy, Aspen Olmsted\"Three Factor Authentication\" Research gate 325078650 |2017.
[10] N. Subash reddy, Ravi Mathey \"Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication\" International Journal of Scientific Engineering and Technology Research ISSN 2319-8885 Vol.03, Issue.50 December-2014, Pages:10187-10189
[11] Miss. Nilima D. Nikam,Mr. Amol P. Pande \"Two Way Authentication System 3D Password-3 Levels of Security\" International Journal of scientific research Volume : 3 | Issue : 1 | January 2014 • ISSN No 2277 – 8179.
[12] B.Madhuravani, Dr. P. Bhaskara Reddy \"A Comprehensive Study on Different Authentication Factors\" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 10
[13] Famutimi Rantiola,Emuoyibofarhe Ozichi,AkinpuleAbiodun,Gambo Ishaya and Odeleye Damilola \"DEVELOPMENT OF A MULTIFACTOR AUTHENTICATION RESULT CHECKER SYSTEM THROUGH GSM\"Computer Applications: An International Journal (CAIJ), Vol.1, No.2, November 2014
[14]Apple. About Face ID advanced technology. https://support.apple.com/en-us/HT208108. (Visited on 02.13.2020).
[15]Apple. About Touch ID advanced security technology. https://support.apple.com/en-us/HT204587. (Visited on 02.13.2020).
[16]https://www.loginradius.com/blog/identity/what-is-multi-factor-authentication/
[17]A. Shamir, ―How to Share a Secret.‖ Communications of the ACM 22.11, vol. 22, no. 11, pp. 612–613, 1979.
[18]Sanjeet Kumar Nayak, SubasishMohapatra, BanshidharMajhi. An Improved Mutual Authentication Framework for Cloud Computing. International Journal of Computer Applications (0975¯8887) Volume 52¯No.5, August 2012. pp: 36-41.
[19]https://www.loginradius.com/blog/identity/what-is-multi-factor-authentication/
[20]https://www.diva-portal.org/smash/get/diva2:1442569/FULLTEXT01.pdf