International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Technical Review of Different Methods for Multi Factor Authentication

Desai Vinanti V[1], Patel Aeny M[2], Ms. Jigna Solanky[3]

[1]*Desai Vinanti V*
[2]*Patel Aeny M*
[3]*Ms. Jigna Solanky, Dept. of computer science, Babu Madhav Institute of Information and Technology, Gujarat, India.*

Abstract - In this paper, we present different methods to authenticate a user. User authentication usually refers to user identification based on something user has, something user is and something user does. Multi Factor Authentication [MFA] is a security system that requirement more than two user credential to identify user for any transactional process. MFA is expected to be utilized for human-to- everything interactions by enabling fast and reliable authentication when accessing service. Multi-Factor Authentication (MFA) was proposed to provide a higher level of safety and facilitate continuous protection of computing devices as well as other critical services from unauthorized access by using more than two categories of credentials.

Keywords – MFA, hand veins, GPS, biometric authentication, passwords, smart card, touch screen authentication.

1. Introduction

Today security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions, etc. Many different types of online services have become available with the development of the internet. Authentication is a process where a "user identifies himself by sending value to the system; the system authenticates his identity by computing and checking that it equals the stored value. MFA verified via the first authentication factor (usually password) along with a second or even a third factor such as smartcards, fingerprints, or user's mouse movements.

Authentication can prevent device and services from authorized access by validating user identity. MFA is an approach for authentication which requires the use of two or more of the universally recognized authentication factors: a knowledge-factor, a possession factor and a biometric factor.

1. *Knowledge factor:*
   - Something the user knows, ex: password
2. *Possession factor:*
   - Something the user has, ex: smart card
3. *Biometric factor:*
   - Something the user is

2. MFA Methods

2.1 Smart card based approach

Nowadays smart card based password authentication has become one of the common authentication mechanism. In this

[1] has used smart based authentication protocol. This protocol includes following phases:

1. Initialization:

   Algorithm for MFA is denoted by (k) -> (PK , SK)

   Where, k = security parameter, PK = Public key, SK = Secret key.

2. Registration:

   In this phase the user data and password will get registered to the system with the use of this protocol.

3. Login-Authentication:

This phase enable the user U to get login to the system successfully with the use of PW, SC and bio-data.

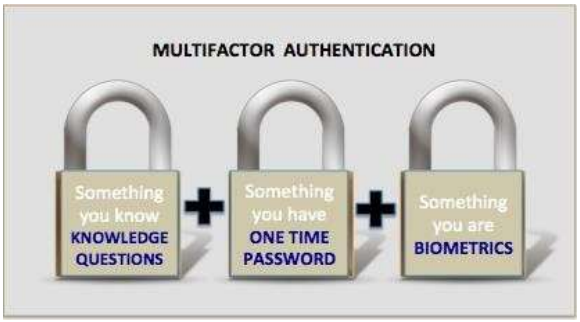
4. Password changing:

This phase will allow the user to change his/her password after a successful authentication. After changing the data, it will automatically updated in the smart card.

5. Bio-metric Changing:

Just like the previous, User can also change their bio-metrics that used in the system.

Ex: Using the different finger user can change their bio-metrics.



2.2 Use of Graphical password

Author of this paper, [2] has used graphical password for user authentication. Graphical password is an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than typing alphanumeric words. This technique is classified into two categories:

1. *Recognition Based:*

In this category, users will select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images.

2. *Re-call Based:*

In this category, users have to reproduce their passwords without being given any type of hints or reminder. Although this category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique.

Table 1: Comparing the security of graphical password and text-based passwords

Issues	Text-Based password	Graphical Password
Dictionary attack	.	
Guessing	.	.
Spyware/key-logger	.	.
Shoulder surfing	.	.

2.3 Method of Risk Assessment

In this paper, [3] author have used different authentication methods for various services. Following services use following methods:

1. Web Portal:

   Log-in, Registration, ID/Password retrieval

2. E-transaction:

   Login, Electronic payment

3. Financial Institution: Login, Account transfer

4. E-government:

   Login, Electronic binding

2.4 Token Presence

In this proposed system [4] has used mobile phone as a software token as s OTP generation for short period of time that are unique. The system will have two modes of operation:

1. **Connection-Less Authentication System:** A onetime password (OTP) is generated without connecting the client to the server.

2. **SMS-Based Authentication System**: The mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone.

The following factors were chosen:

1. **IMEI number**: It stands for International Mobile Equipment Identity which is unique to each mobile phone allowing each user to be identified by his device.

2. **IMSI number:** It stands for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System.

3. **PIN:** This is required to verify that no one other than user can use the phone to generate the user's OTP.

2.5 MFA using PGT

The author [5] has use PGT [Preshared number, GPS Location and Time Stamp] that enhances security by generating a secret hash code based on a pre0-shared number and user's current GPS location.

The GPS location utilizing the device's geographical location to validate whether access to the device/service could be granted is a special case of location-based authentication. GPS signal could be easily jammed or considered faulty due to the propagation properties. Thus, it is recommended to utilize at least two location sources ,for example, GPS and wireless network cell ID.

PGT Authentication Scheme

Stage 1:

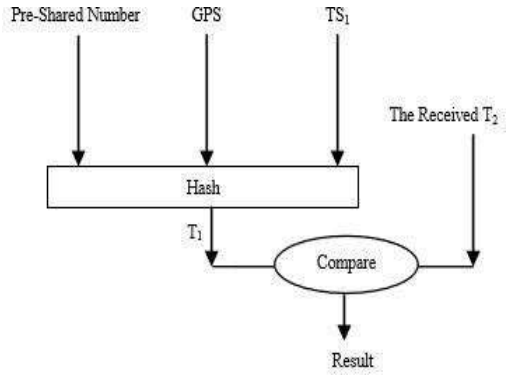
Stage 2:

In this stage app is responsible for generating the security token T1 according to the following equation where TS1 is the current time stamp:

T1=hash (Pre-Shared Number + GPS + TS1);

Stage 3:

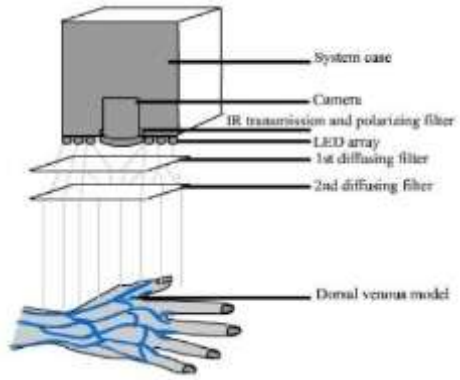
Server generates a security token T2 using equation1. Then it compares T1 with T2, if they match, the user is authenticated and his personal web page is sent back to device.



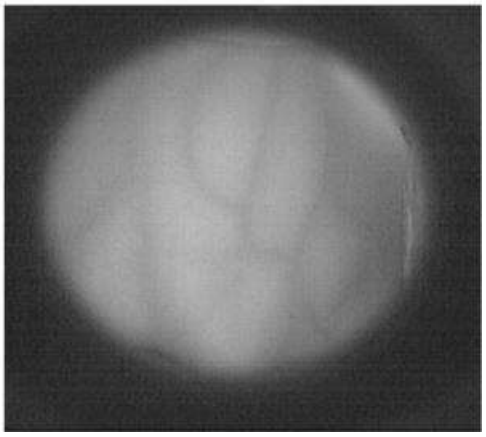
2.6 HandVeinRecognition

The authors [6] of this method, has used touch sensing system. One of the most user identification system is **DiamondTouch** by *Mitsubushi Electric Research Laboratory.* The system use a top mounted camera to track the user's hand on the tactilesurface.

In this stage, the user requests his personal web page URL through any internet- enabled device. The user provides his credentials to device which sends them to server for verification. If the user is verified, server asks for the security token.



In this method close touches from different hands are hard to identify. This method will let user to identify by lying their hand on the surface. Lighting should be perform under a very tight optical window in the range of 750-940 mm. It acquire the pattern of the back of your hand. The below image do a transformation that extract the vein pattern.



2.7 DNA Recognition

Human cell lines are an essential source of unique DNA fingerprinting information. Even though the process is time-consuming and expensive, it provide highly secure facility as compare to other factors.

The factors evaluated for the comparison of suitable factors for MFA are as below:

- Universality: the presence of factor in each person.
- Uniqueness: how well the factor differentiates one person from another.
- Collectability: how easy it is to acquire data for processing.
- Performance: the achievable accuracy, speed, and robustness.
- Acceptability: the degree of acceptance of the technology by people in their daily life.

2.8 Using Biometric Authentication

Authentication is one of the most important issue in computer security management and information system. In biometric authentication such as fingerprint, handwriting, signature, or characteristics of user behaviours.

Other biometric authenticationa are retina authentication, hand-gesture authentication, human body print authentication as well as the characteristics behaviours such as movement and keystroke authentication. This type of authentication are more secure then fingerprint.

In that two methods are involved:

- **Namely ,physical biometric:**

  It is uses human body parts such as fingerprint, retina, face,DNA and hand geometry.

- **Behavioral biometric:**

  It is uses measurable patterns in human activities such as keystroke dynamic, voice ID and gait analysis.

The performance of biometric authentication can measure three factor include:

- **False Acceptance Rate(FAR):** It is the measure of possibility that the biometric incorrectly permit an access attempt by an unauthorized user.
- **False Rejection Rate(FRR):** It is the measure of the likehood that the biometric incorrectly denies an access attempt by an authorized user.
- **Equal Error Rate(EER):** When FAR and FRR are equal, it is called EER.

2.9 Using Key mangment :

In this PKI(Public Key Infrastructure) based on e-health authentication architecture.It is stores user credentials and digital certificates in smart cards to provide a strong authentication method.

- **Client and server:**

The KMS will be responsible for authenticating and authorizing the user to use cryptographic keys to create signature or to maintain the electronic data.it will work as a secure cryptoprocessor, maintain the correct execution.

- **One time password:**

The principle of OTP is to sharea seed between a generator and a verifier where produce the same number.

- **Diffie-Hellman Key Exchange:**

The main porpose of sharing a secret though a public network and we used it to share the seed of the OTP protocol.

- **QR code:**

The QR code was invented by the Japanese corporation denso wave.the QR code makes the intraction between mobile devices and other data formats easier.

3. Literature Review

In paper [5], This paper presents a new mobile-based multi-factor authentication scheme based on a pre-shared number, GPS location and Time stamp (PGT).A new multi- factor authentication method was presented. It utilizes the user's mobile device to generate an OTP which can be used as an authentication second factor. Unlike other methods of multi- factor authentication that employ the use of special devices like a security token which adds more cost to the authentication system, PGT uses a mobile device which is a common device for all users.

It generates a security token T2using equation . Then it compares T1 with T2 , if they match, the user is authenticated and his personal web page is sent back to D1.It increases the security risk as the shared seed can be intercepted by an intruder. Also the OTP does not contain user specific information like the user's current GPS location which makes it less powerful compared to our proposed approach.

In paper [4], This paper focuses on the implementation of two-factor authentication methods using mobile phones. It provides the reader with an overview of the various parts of the system and the capabilities of the system.The proposed system has two option of running, either using a free and fast connection-less method or a slightly more expensive SMS based method. Both methods have been successfully implemented and tested, and secure.Such programs implement a One Time Password (OTP) algorithm. OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in thesequence.

The proposed system has two option of running, either using a free and fast connection-less method or a slightly more expensive SMS based method.

In paper [10], Multi-factor authentication is utilized for human-to- everything interactions by enabling fast, user-friendly, and reliable authentication when accessing a service.In MFA many method or source are available but in this paper DNA recognition method is used and in that Human cell lines are an essential resource for research, which is most frequently used in reverse genetic approaches.It is also a source of unique DNA fingerprinting information. Even though the process is time-consuming and expensive, it may be potentially utilized to pre-authorize the user to the highly secure facility along with other factors.

In paper [7],in this method system is not to implement and provide its own, proprietary authentication factors but to enable transparent access to authentication factors provided by third parties. The basic requirement for the MFAS is the capability to connect and use all of the above mentioned authentication mechansims. The function of the MFAS is reduced to facilitating the authentication server in providing an online user interface. Some authentication factors perform a local verification of credentials on the user device or an attached/connected device and expose the authentication results so that they can be used by the MFAS.

In paper[8], Authentication is one of the most important issues in computer security management and information systems. The biometric authentication that is widely used is fingerprint authentication . Fingerprint can be used to access a personal computer, access a smart phone.

Keystroke authentication may be an alternative since it is not costly and easy to implement. In Biometric authentication unique biological characteristics of individuals to determine identity, which consists of two methods, namely, physical biometric and behavioral biometric.It can prevent shoulder surfing attacks. This is because users do not need to look at their keyboard when tapping or touching a touchpad or a touch screen.

In paper[2], the user enters the password by clicking on a set of images, specific pixels of an image,or by drawing

a pattern in a pre-defined and secret order. graphical password employs graphical presentations such as icons, human faces or custom images to create a password .Our approach can be effectively and securely used as user-friendly authentication mechanism for public and un-trusted users.

In paper[1], we demonstrate how to incorporate biometrics in the existing authentication based on smart card and password. smart-card-based password authentication has become one of the most common authentication mechanisms. simple dictionary attacks can crack passwords in a short time.A solution to preserve user privacy even the server has a copy of clients' biometric data.the store data and the input biometric data.

In paper[6],A biometric system is a pattern-recognition system that recognizes a person vein pattern and uniqueness of the vein pattern. detecting various subject even twin or distinguish vein model in both hand from the same user.Vein pattern recognition with a suitable optical system.when comparing these methods the biometric model is compatible with the optical sensing device that allows object and pattern detection on surface.

Table2: Comparison of suitable factors for MFA: H—high; M—medium; L—low; n/a—unavailable.

Factor	Universality	Uniqueness	Collectability	Performance	Acceptability
Password	n/a	L	H	H	H
Token	n/a	M	H	H	H
Voice	M	L	M	L	H
Facial	H	L	M	L	H
Fingerprint	M	H	M	H	M
Hand – geometry	M	M	M	M	M
Location	n/a	L	M	H	M
Vein	M	M	M	M	M
Behaviour	H	H	L	L	L

4. Comparative Study of Different Methods for MFA

NO	Methods	Performance	Application	Advantage	Disadvantage
1	retina authentication hand-gesture authentication,heart rate authentication,human body print authentication	The performance of biometric authentication can measure three factor:False Acceptance Rate(FAR),False Rejection Rate(FRR),Equal Error Rate(ERR).		it is not costly and easy to implement	They are more expensive.
2	Token presence	Each token has a unique seed which is used to generate a pesudo-random number.this seed is loaded into server upon purchase of the token and every 60 second.	Gmail, WhatsApp	imporving capabilities of mobile devices.	it include the cost of purchasing ,issuing and managing the token or cards.
3	Graphical password	this method can effectively address the gussing and shoulder-surfing issue of other image-password method	google re-capcha	this approch overcome the limitation of the traditional password system.	
4	Smart Card based	This method proposed to improve the information assurance at low cost but also protect client privacy in distributed system.	OTP	Improve the information assurance in distributed system and improve security feature	
5	hand vein recognition	this system use for pattern-recognition system that recognizes a person specific physiological behavioral charactristic that the person processes.	Financial application(ATM), Health care application,Employee time recording /access control.	identification number and password since the risk of identifying theft and other security concerns.	hand contour detection has a low discrimination ratio in camparison to other biometric techniques and night provide an increased number of false acceptance.

6	Pre-shared number.GPS location and time stamp	it is stores credential and digital certificates in smart cards to provide a strong authentication method.		PGT is less expensive and more secure.	GPS location which makes it less powerful campared to our proposed approch.
7	Network based authentication ,local authentication	This all approach pose a security risk in reducing the effectiveness or strength of an authentication.		It is very flexible and simple authentication .	

5. Conclusion

In this paper we proposed a new authentication scheme based on different MFA methods. Our approach can be effectively and securely used as user friendly authentication mechanism for public and untrusted terminals. Preserving security and privacy is challenging issue in distribute system. In this review paper we have study different types of methods and compare different types of methods. Table 1 contains comparison of text based password and graphical password. Table 2 contains comparison of different methods.

6. Reference

1. Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three- factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems, 22(8), 1390-1397.

2. Sabzevar, A. P., & Stavrou, A. (2008, November). Universal multi-factor authentication using graphical passwords. In 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems (pp. 625-632). IEEE.

3. Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication.Journal of Information Processing Systems, 7(1), 187-198.

4. Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 641-644). IEEE.

5. Abdurrahman, U. A., Kaiiali, M., & Muhammad, J. (2013, November). A new mobile-based multi- factor authentication scheme using pre-shared number, GPS location and time stamp. In 2013 International Conference on Electronics, Computer and Computation (ICECCO) (pp. 293-296). IEEE.

6. Crisan, S., Tarnovan, I. G., Tebrean, B., & Crisan, T. E. (2011). Hand vein biometric authentication in optical multi-touch systems. In International Conference on Advancements of Medicine and Health Care through Technology (pp. 124-127). Springer, Berlin, Heidelberg.

7. Huang, X., Xiang, Y., Bertino, E., Zhou, J. and Xu, L., 2014. Robust multi-factor authentication for fragile communications. IEEE Transactions on Dependable and Secure Computing, 11(6), pp.568- 581.

8. Wongnarukane, N. and Kuacharoen, P., 2016, December. Rhythm Authentication Using Multi- touch Technology: A New Method of Biometric Authentication. In International Conference on Smart Computing and Communication (pp. 390-399). Springer, Cham.

9. De Souza, R.L., Lung, L.C. and Custódio, R.F., 2013, July. Multi-factor authentication in key management systems. In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 746-752). IEEE.

10. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018. Multi-factor authentication: A survey. Cryptography, 2(1), p.1.