# Transaction Authentication Methods – A Survey

V. B. Swedha[1],
Department of Computer Science and Engg,
S. A. Engineering College,
Anna University, Chennai, India

K. Priyadarshini[2]
Assistant Professor,
DMI College of Engineering,
Anna University, Chennai, India

***Abstract*— Now-a-days everything is accomplished through online. Mutual transfers between users or companies or a customer and concern needs to be authenticated at other end. There enters transaction authentication for each exchange done on Internet. In online transfers both the entities are anonymous and not be viewed face to face, but they have to trust each other mutually. The integrity of this business should be maintained. Based on requirement of the web service provider has to decide on the level of security. According to sensitive data, that transferred online may choose relevant authentication method. This paper surveys various authentication methods for online transactions. Each scheme is defined with terms. Finally, concluded with a comparison chart about the security provided by each authentication type.**

***Keywords*— Authentication, Web Service, Online transaction.**

## I. INTRODUCTION

Online transaction defines an operation that takes place from one machine to a server in the form of request and response. The server immediately replies to user requests. Here user is not physically stand before the server, through a network connection the user communicates with server. So the user should be authenticated for the server to satisfy the specific user request.

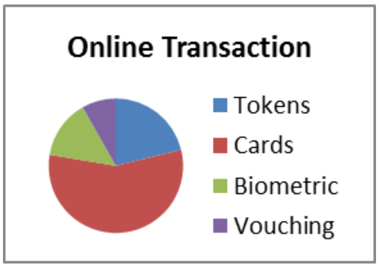

Fig. 1 Usage of Online Transaction Authentication Methods

An authentication is a process of giving identity to persons involved in a business. In online transaction like banking sector, bank has to authenticate account holders with a login identity and password. Each transaction done by customer should be verified and password protected, other online transactions like shopping, shares, etc., ends at banking transaction. Intruders or adversaries are also mostly interested with financial data. They try to hack the user id and password. There are different types of attackers tries to hack different things. Say for example user personal information, credit card details, passwords, etc,.
Authentication relies upon four factors

- Something the user knows (Knowledge factor)
- Something the user has (Ownership factor)
- Something the user is (Inherence factor)
- Something the location of user (Mobility factor)

These factors [1] can stand alone for the authentication or they may combine as more than one. As a single factor authentication, it can be easily hacked, when more than one factor joined then breaking the authentication system become complicated. So it can provide more security.

In face-to-face transaction, the account holder can easily access the account without any identity. But in the online transactions, the account holder should prove that he belongs to the account and he only making the operation. This is a unbeaten challenge faced in those transactions.

## II. FACTORS OF AUTHENTICATION

In the beginning of web world the authentication deals with single or two factors. Now, advanced technology running with four factors.

### *A. Knowledge Factor*

Knowledge factor is the simplest authentication method. Password is a collection of characters treated as secret word. This secret word used as authentication tool. Pattern is a sequence of strings used for user authentication. This pattern are used in Android mobile devices. PIN is Personal Identification Number contains numeric digits used in debit or credit cards.

### *B. Possession Factor*

In ancient days the most popular authentication factor is possession factor. This factor is like lock and key. The lock act as authentication device and user tries to enter will have the exact key for that lock. Only the person who keeps the key can unlock the device.

TABLE I
COMPARISON OF AUTHENTICATION FACTORS

| **Factors** | **Example** | **Vulnerable** | **Cost** | **Security** |
|---|---|---|---|---|
| *Knowledge* | Password, PIN | Brute force attack, Dictionary attack | Less expensive | Low secure |
| *Possession* | Cards, Tokens | Man-in-the-Middle attack, Session fixation, Side jacking | Medium, expensive if hardware used | Secured |
| *Inherence* | Biometric | Replay attack | Expensive | Highly secured |
| *Mobility* | Mobile location | Cyber Threats | Very Expensive | Secured |

### *C. Inherence Factor*

A characteristic that unique to the user is inherence factor. Biometric act as inherence factor in authentication method, is a combination of more than one factor. Users authenticate through their iris scan, fingerprints, and facial images or audio that can be done with hardware device and PIN or password with software. This type of authentication is expensive because of hardware device and combining more than one factor. It is vulnerable to replay attack. If any of the biometric information is compromised then the account is easily prone to replay attack.

### *D. Mobility Factor*

Other than the three well known factors, the fourth factor denotes where you are. The location of the user is identified through the mobile device or any other equivalent device helps to locate the user existence. The location of the user taken as the fourth factor. It provides high level security. The location of the mobile device is tracked and identified the place of user, then the transaction will be validated according to the user location and browser location.

## III. EXISTING SYSTEM

The systems that are using user login and password follows different methods of authentication. Many applications uses the password system which make the user in more heaviness. Latest methods are trying to eliminate human work and making automatic authorization process. Some of them are discussed here.

### *A. Single Factor*

Passwords are used as single factor for authentication in many applications. Most of the passwords or PIN are the combined with other authentication factors. Drawbacks of passwords are, maintaining the level of passwords at admin level, easily guessable, frequent change of passwords, users may note down password in common places.

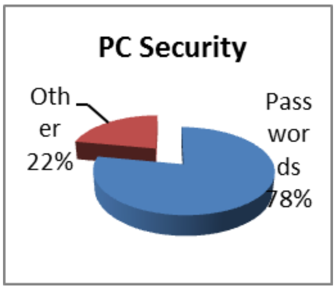

Fig. 2 Percentage of Password as Authentication Factor in Personal Computers

Passwords are mostly used in personal computers. To secure the computer terminals the password will be acting as authentication tool. Other types of security measures are also available, but passwords occupy 78% of systems or laptops.

In Fig. 2, the percentage of passwords used as authentication for the personal computers is shown. Still the computer devices rely upon passwords as their primary security. Passwords are used quarter of the total authentication methods. The remaining others consist of finger print, voice, iris, graphical images, facial, etc,.

### *B. Two Factor*

Two factors authentication provides more security than single factor. The two factors can combine PIN with credit or debit cards. Passwords are combined with tokens. Single factor of authentication [2] can by weakened by software attacks.

In industries for business purpose, the authentication factors occupies as major contribution by two factor method, next one is one factor and then three factor. The three factor authentication type is expensive than other two.

TABLE III
COMPARISON OF AUTHENTICATION SYSTEMS

| **Authentication type** | **Industries** | **Devices (Laptop, Mobile, PC)** | **Online Transaction** | **Merits** | **Demerits** |
|---|---|---|---|---|---|
| **Password** | Preferable for devices | Mostly used | In different forms like OTP, PIN | Inexpensive, Easy to install | Need Database to store Passwords, Complex to maintain, Less secured |
| **Smart Cards** | Used for employees | Used with organisations | Mostly used here | Secured | Smart card reader needed |
| **Biometrics** | Broadly used | Very less | Less applications | More secured | Expensive |
| **Mobile Phones** | Not much | Not much | Used in many applications | Secured | Less expensive than biometrics |

### *C. Tokens*

There are two types of tokens.

- *Software Token*

  A software is designed to generate tokens for authentication. For example to access an application, the token will be acting as the authentication factor for the user. In GitHub, there was an option in applications to create new token. This token will act like password to access Git API. Another software based token is soft tokens. Soft tokens maintains banking credentials on mobile devices and on computers also.
- *Hardware Token*

  There are many hardware tokens like USB tokens, audio port tokens, RFID based tokens, Bluetooth based tokens, contactless smart cards. USB tokens have a huge storage capacity to store login details. Audio port tokens are used as authentication tool for mobile phones and laptops. Generally hardware tokens are costlier than software.
- Another type of token called Enhanced tokens [3] contains multi-function smart cards that can store multiple passwords on a single token. So more than one action can be performed with same smart card.
- Tokens faces another challenge is its battery power. The existing tokens that can withstand for 5 to 7 years. The battery lifetime of tokens as minimum of 5 years and maximum of 7 years.

### *D. Smart Cards*

Latest authentication method in the smart cards is dynamic authentication with sensory information [4]. Before the control systems are accessed through the authentication done with encoded identification information stored in access card. The drawback of the scheme is card loss and unauthorized duplications. The new model that contains sensory information obtained from wireless rechargeable sensors on access cards for further enhancement of security and robustness.

Microsoft operating system has smart card based authentication. The card is authenticated against password and can be unlocked using smart card device driver. It used to lock and unlock computers.

A hardware token type smart cards used in some organizations which consist of an ISO, display, button and non-rechargeable battery. When button pressed One Time Password (OTP) will be generated.

The smart cards may prone to any of the following attacks.

- ID Spying:

  The legitimate user details may be hacked through keyloggers. While user typing the information, it may be hacked by adversaries
- First party fraud:

  The legitimate user may purposefully not to pay the credit card payment.
- Counterfeit fraud:

  The duplicate of card is made by adversaries and tries to act as like legitimate user.

### *E. Biometrics*

As biometrics aims to recognize a person using unique features of human physiological or behavioural characteristics such as fingerprints, voice, face [5], iris, gait and signature, this authentication method naturally provides a very high level of security. Conventionally, biometrics works with specialized devices, for example, infrared camera for acquisition of iris images, acceleration sensors for gait acquisition and relies on large-scale computer servers to perform identification algorithms, which suffers from several problems including bulky size, operational complexity and extremely high cost.

Biometrics plays a challenging role in various industries, from medicine, science, robotics, engineering, manufacturing, etc,. It provides individual privacy for different users. Use of biometric authentication has increased among enterprises. The different forms of biometrics pose problems like voice recognition will work on specific voice types, fingerprint recognition work of particular fingers. Latest systems use multiple biometric factors like, facial recognition with voice and lip movement.

Face recognition was a familiar authentication method. Latest technology in face recognition is authenticating the user even they are with different make-ups.

Fingerprint biometric [6] has been adopted widely for access control in places requiring high level of security such as laboratories and military bases. By attaching a fingerprint scanner to the mobile phone, this biometric could also be utilized for phone related security in a similar manner.

### F. *Multifactor*

Latest technologies uses multifactor authentication. Mostly the three factors are used in online transactions [7]. In the figure 3, the percentage of single factor, two factor and three factor. The devices that involved are device drivers, card reader and mobile phones.

The figure denotes the industries that opts for the possibility among three factors.

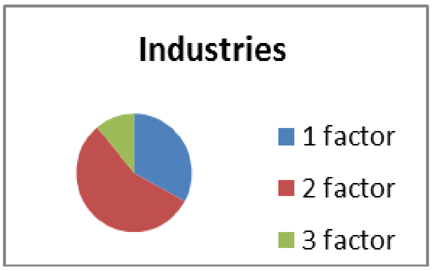

Fig. 3 Industries opting for Factor Authentication

### G. *iTPS*

An insider Threat Prevention System [1] is an application that uses the forth factor of authentication. This application uses RTLS (Real Time Locating System) for tracking materials and personnel. The technology checks the user location before giving access to the request for the system. Its more secure and there won't be any miss-happen takes place.

## IV. Future Online Banking

Future online banking [8] can also combine more than one factor, ie; multifactor authentication. Even though the multifactor authentication is prone to attacks, since this will enhance the security system in the specific applications. Analysts predict that the spending by banks on anti-fraud solutions will grow at about 30% over the next few years. When industries selecting the authentication method, they encounter level of security achieved and investment which should be less than what they earn.

## V. Conclusions

This paper analyses the different authentication mechanisms for online transactions. Here the evaluation of each method is scrutinized and figured out for the specific applications. Choosing right authentication method is a challenging process, which decides whole system security. The two table comparison helps to find the factor related details and existing system information. The survey guides the application users to select respective authentication method based on their requirement mainly concentrating on cost and security.

## Acknowledgment

The authors thank the anonymous reviewers for their helpful suggestions to improve the paper.

## References

[1] Sing Choi and David Zage, "Addressing Insider Threat using Where You Are as Fourth Factor Authentication", The 46th Annual IEEE International Carnahan Conference on Security Technology, 2012.

[2] Richard P. Guidorizzi, "Security: Active Authentication", *IEEE Computer Society,* IT Pro July/Aug, 2013.

[3] Dr. Jucheng Yang, "Biometrics on Mobile Phone", *Publisher in Tech,* ISBN 978-953-307-488-7, July, 2011.

[4] Yuanchao Shu, Yu Gu and Himing Chen, "Dynamic Authentication with Sensory Information for the Access Control Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No.2, 2014.

[5] Guodong Guo, Lingyun Wen and Shuicheng Yan, "Face Authentication with Makeup Change",, *IEEE*, 2013.

[6] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication ", *IEEE Transactions On Information Forensics And Security*, Vol. 8, No. 1, January 2013.

[7] Lawrence O'Gorman, "Securing Business's Front Door – Password, Token, and Biometric Authentication ".

[8] T. C. Dinesh, "What the Future of Online Banking Could Be", Perspective, Finacle from Infosys, 2011.